Veiligheid en Privacy in 2030

Koops, E.J.; Poels, R.C.P.; Leenes, R.E.; Lips, A.M.B.; Prins, J.E.J.; Vedder, A.H.; Groenhuijsen, M.S.

Publication date:
2005

UNIVERSITEIT VAN TILBURG

Veiligheid en privacy in 2030: twee toekomstscenario's

Bert-Jaap Koops
Rachel Poels
Ronald Leenes
Miriam Lips
Corien Prins
Anton Vedder
Marc Groenhuijsen

TILT – Centrum voor Recht, Technologie en Samenleving

Januari 2005

Centrum voor Recht, Technologie en Samenleving
Postbus 90153 • 5000 LE Tilburg • Bezoekadres > Warandelaan 2 • Tilburg • Telefoon 013 466 81 99 • www.uvt.nl/tilt/

Inhoudsopgave

1. Inleiding

1.1. Aanleiding

Deze studie is geschreven in opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. De opdracht betrof het schrijven van twee toekomstscenario's voor Nederland in 2030 waarin privacy en veiligheid verschillende nadruk krijgen. Op basis van deze toekomstscenario's zouden beleidskeuzevragen moeten kunnen worden geformuleerd.

1.2. Doel en vraagstelling

Het *doel* van deze studie is: twee – extreme maar denkbare – toekomstbeelden van de Nederlandse maatschappij in 2030 te schetsen, één waarin veiligheid meer centraal staat en één waarin privacy meer centraal staat, die kunnen worden gebruikt om strategische beleidskeuzes te maken inzake het spanningsveld tussen veiligheid en privacy.

De *vraagstelling* die centraal staat is: hoe kan de Nederlandse maatschappij er in 2030 uitzien, gegeven te verwachten technische ontwikkelingen, waarbij in beleid en wetgeving de komende decennia bij noodzakelijke afwegingen tussen veiligheid en privacy structureel de meeste voorkeur wordt gegeven hetzij aan veiligheid, hetzij aan privacy?

1.3. Afbakening

De vraagstelling is breed. Aangezien deze studie geschreven is in een betrekkelijk korte periode van drie maanden, met bovendien een beperkte onderzoeksomvang, zijn er de nodige keuzes gemaakt ter inperking van de studie. Wij hebben ervoor gekozen de beperking deels te zoeken in de onderzoeksopzet (zie par. 1.4) en deels in de reikwijdte van het onderzoeksobject. Wij hebben niettemin getracht het onderzoeksobject breed te houden, omdat de nadruk ligt op verkenning en het oproepen van vragen en niet op een precieze aanduiding van specifieke problemen.

techniek

De toekomstbeelden rond veiligheid en privacy worden grotendeels belicht vanuit de *techniek*. De reden voor deze keuze is dat veel technische ontwikkelingen grote invloed op privacy en veiligheid en op het spanningsveld daartussen. Het perspectief van techniek biedt dan ook een interessante en relevante blik waarmee de toekomst bekeken kan worden. Binnen het domein van techniek hebben wij de nadruk gelegd op technologieën die maatschappelijk relevante toepassingen zullen opleveren, zoals privacybevorderende techniek (PETs) en toezichtbevorderende techniek (Surveillance Enhancing Technologies, SETs). Hierbij is gekeken naar informatie- en communicatietechnologie (ICT), biotechnologie, nanotechnologie,[1] robotica, en combinaties van een of meer deze technologieën. Het onderzoek is aldus geconcentreerd op veiligheids- en privacyontwikkelingen die samenhangen met deze technologieën, om het onderzoek hanteerbaar te houden en de scenario's scherp te kunnen stellen door de maatschappij te belichten vanuit het perspectief van technische (on)mogelijkheden.

De manier waarop waardennoties als veiligheid en privacy in de ethiek en in het recht geconceptualiseerd worden is sterk afhankelijk van maatschappelijke en culturele omstandigheden. Daarom is te verwachten dat de invulling van wat men verstaat onder veiligheid en privacy in 2030 in hogere of mindere mate zal verschillen van de huidige invulling. Aangezien de doelstelling van het onderzoek evenwel is om beleidskeuzes te faciliteren die in het huidige tijdperk relevant zijn, hebben wij ervoor

[1] Nanotechnologie is gericht op het maken van systemen op een schaal van 1 tot 100 nanometer (1 nm = één miljardste meter). Deze systemen worden opgebouwd uit individuele atomen, en kunnen bijvoorbeeld worden ingezet in kunstmaterialen en in biotechnologische toepassingen binnen het lichaam.

gekozen om bij veiligheid en privacy uit te gaan van de huidige noties van deze begrippen.

veiligheid In deze studie wordt daarom uitgegaan van een tamelijk conventioneel *veiligheidsbegrip*. In essentie houdt dit in dat burgers het gevoel willen hebben dat zij op adequate wijze worden beschermd tegen onrechtmatige of disproportionele inbreuken op lijf, eerbaarheid en goed. De meest in het oog springende van dergelijke inbreuken zijn de klassieke delicten uit het commune strafrecht: geweldsdelicten, vermogensdelicten en zedendelicten. Voor het domein van veiligheid beperkt het onderzoek zich tot drie verschijningsvormen die nauw verbonden zijn met dit veiligheidsbegrip: kleine criminaliteit (zoals winkeldiefstal en inbraak), zware criminaliteit (zoals georganiseerde wapenhandel en moord) en terrorisme.

privacy Verder wordt in de scenario's uitgegaan van het huidige *privacybegrip*. Dit betekent dat ten aanzien van privacy wordt uitgegaan van een begrip dat net als nu vier dimensies heeft: informationeel (bescherming persoonsgegevens), fysiek (integriteit van het lichaam), ruimtelijk (relatieve onschendbaarheid van de woning en persoon in openbare ruimte) en relationeel (relaties, gezin, communicatie).

geen tegenpolen Overigens moet worden opgemerkt dat privacy en veiligheid lang niet altijd tegenpolen zijn, maar elkaar vaak ook kunnen versterken.[2] In de onderhavige studie worden dergelijke 'win-win-situaties' bewust onderbelicht; het onderzoek concentreert zich, zoals de vraagstelling luidt, op *noodzakelijke* afwegingen tussen veiligheid en privacy, en dus op onderwerpen waarbij de keuze voor veiligheid enigermate gepaard zal gaan met aantasting van privacy, en omgekeerd. Daardoor zullen de scenario's maximaal onderscheidend kunnen zijn en meer openingen bieden voor beleidskeuzes. Aangezien het echter een grove vertekening van de werkelijkheid zou zijn veiligheid en privacy als fundamenteel tegengestelde doeleinden te zien, bevatten de scenario's ook enkele voorbeelden waarin de keuze voor veiligheid en de keuze voor privacy juist samengaan.

1.4. Methodologie

typering scenario's De beperkte omvang van het onderzoek legde beperkingen op aan de methoden die konden worden gehanteerd om tot toekomstbeelden te komen. Gekozen is voor een scenario-onderzoek dat, in de typologie van Van Notten e.a., kan worden getypeerd als beslissingsondersteunend, intuïtief-kwalitatief en complex.[3] Meer specifiek kan dit scenario-onderzoek worden getypeerd aan de hand van de volgende karakteristieken:[4]

- doel:
  - *beschrijvend*: de toekomstbeelden beschrijven mogelijke toekomsten, niet wenselijke toekomsten;
  - *vooruitblikkend*: vanuit het heden wordt gekeken hoe de toekomst zich zou kunnen ontwikkelen;
  - *onderwerp-gebaseerd*: de beelden belichten de onderwerpen veiligheid en privacy;
  - *lange termijn*: de beelden kijken ver vooruit, naar 2030;
  - *nationaal*: de beelden beschrijven Nederland;
- opzet:
  - *kwalitatief*: de toekomstbeelden zijn kwalitatief en in verhalende vorm, niet kwantitatief;
  - *expertonderzoek*: de bestanddelen van de toekomstbeelden zijn grotendeels afkomstig van visies van experts (de onderzoeksgroep

[2] Zoals ook opgemerkt in vraaggesprekken (bijlage I) en door diverse respondenten (bijlage II).
[3] Van Notten e.a. 2003, p. 426-428.
[4] Van Notten e.a. 2003, p. 429-434.

aangevuld met diverse domeindeskundigen); deze gegevensbron is aangevuld met literatuuronderzoek;
    - *beperkt*: voor het onderzoek zijn beperkte middelen beschikbaar;
    - *open*: het onderzoek kent geen institutionele of beleidsbeperkingen die de scenario's inhoudelijk sturen;
- inhoud:
    - *momentopname*: de beelden geven geen ontwikkeling in de tijd, maar een momentopname uit 2030;
    - *heterogene variabelen*: de toekomstbeelden gaan uit van een multifactoriële, complexe omgeving waarin vele heterogene variabelen tezamen een rol spelen;
    - *extrapolatie*: de toekomstbeelden zijn in beperkte mate contrastrijk of verrassend ten opzichte van de huidige maatschappij; zij zijn grotendeels gebaseerd op tendensen uit 2004 die worden geëxtrapoleerd, vanwege de dienende functie van de toekomstbeelden voor beleidsscenario's;
    - *alternatieve scenario's*: er worden twee toekomstbeelden geschetst die onderling contrasteren;
    - *integratie*: de beelden proberen de diverse variabelen tot op zekere hoogte te integreren door hun interactie te verweven in samenhangende verhaallijnen.

bronnen Naast wetenschappelijke en vakliteratuur is als gegevensbron gehanteerd de expertise van de onderzoeksgroep op het terrein van veiligheid, privacy en techniek, die gestoeld is op jarenlange onderzoekservaring op dit gebied (zie Bijlage III met beschrijving van de onderzoekers). Voorts is substantiële inbreng geleverd door vraaggesprekken met vier experts op de terreinen van veiligheid, privacy en techniek, te weten Ybo Buruma (veiligheid), Erik Huizer (ICT), Ulco van de Pol (privacy) en Arie Rip (nano- en biotechnologie) (zie bijlage I met verslagen van deze vraaggesprekken). Deze gegevensbronnen zijn aangevuld met inbreng via een webvragenlijst; diverse mogelijke respondenten uit wetenschap, publieke sector (ministeries en magistratuur) en lezers van ICT-recht-gerelateerde nieuwsbrieven zijn uitgenodigd de vragenlijst in te vullen; een twintigtal (anonieme) respondenten heeft hieraan gehoor gegeven. Een samenvatting van deze reacties is te vinden in Bijlage II.

1.5. Opzet

Dit rapport gaat uit van twee toekomstbeelden, één waarin de maatschappij sterke nadruk legt op veiligheid (in het vervolg ook aangeduid als 'veiligheidsmaatschappij') en één waarin de maatschappij sterke nadruk legt op privacy (in het vervolg ook aangeduid als 'privacymaatschappij'). De invulling van deze toekomstbeelden is gebaseerd op verwachtingen ten aanzien van ontwikkelingen in veiligheid, privacy en techniek.
In deel I worden eerst deze ontwikkelingen geschetst. Achtereenvolgens komen ontwikkelingen in de samenleving aan de orde, die dienen als achtergrond waartegen de twee toekomstbeelden zich afspelen (hfd. 2), ontwikkelingen in techniek (hfd. 3), veiligheid (hfd. 4) en privacy (hfd. 5). Vervolgens worden in deel II twee verhalende toekomstbeelden geschetst, in een luchtiger stijl, één van een veiligheidsmaatschappij (scenario A) en één van een privacymaatschappij (scenario 1).

kanttekening Wie zich tot doel stelt twee scenario's te schetsen, waarbij het ene vertrekt vanuit veiligheid en het andere vanuit privacy, wordt als vanzelf geconfronteerd met de omstandigheid dat veiligheid een tamelijk concrete notie is, terwijl privacy voor een complexe waarde of wellicht zelfs een complex agglomeraat van waarden staat. Daarbij komt dat privacyoverwegingen een sterk "troefkaart-karakter" hebben. Dat wil zeggen dat zij eerder hun werk doen als beperkende condities bij door andere overwegingen (zoals veiligheid of algemeen belang) gemotiveerd beleid, dan dat zij zelf tot zelfstandig beleid aanleiding geven. Hoewel het altijd moeilijk is om enkele

decennia vooruit te kijken, biedt het veiligheidsperspectief hierdoor meer aanknopingspunten dan het privacyperspectief. Om deze reden is als insteek van de twee scenario's gekozen voor de volgende opzet. Bij de ontwikkelingen wordt telkens voor een aantal variabelen gevarieerd tussen de twee scenario’s. Hierbij wordt steeds begonnen met veiligheid als betrekkelijk duidelijke, inhoudelijke factor die sturing kan geven aan een maatschappij; vervolgens wordt ingegaan op privacy als beperkende, afgrenzende factor. In deze opzet komt het verschillende karakter van veiligheid en privacy naar voren: men kan goed een beeld schetsen van een maatschappij waarin veiligheid de heersende richtinggevende factor is, maar minder goed een beeld van een maatschappij die zich alleen laat leiden door privacy. In die zin fungeert het veiligheidsscenario als vertrekpunt.

Deel I. Achtergronden en ontwikkelingen

2. Samenleving

2.1. Maatschappelijke context en ontwikkelingen

Bij de scenariovorming gaan wij uit van maatschappelijke ontwikkelingen die in het verlengde liggen van huidige en nu voorzienbare tendensen. Deze ontwikkelingen zijn aangedragen door de opdrachtgever, gebaseerd op diverse sociologische verkenningen, en aangevuld met enkele observaties uit andere bronnen. Tezamen vormen deze ontwikkelingen de maatschappelijke context voor de privacy- en veiligheidsscenario's.

staat

Nederland blijft als land bestaan. Dat wil zeggen dat we ervan uitgaan dat Nederland niet door een stijgende zeespiegel in de Noordzee verdwijnt en evenmin wordt getroffen door een meteorietinslag. Staatkundig zal Nederland nog een zelfstandige eenheid van betekenis vormen, al dan niet binnen een Verenigde Staten van Europa. Europa heeft weliswaar een toenemende invloed, maar de nationale overheid bepaalt nog steeds substantiële onderdelen van gebieden als sociale zekerheid, veiligheid, openbaar bestuur en infrastructuur.
Het *politieke systeem* blijft in zijn huidige vorm herkenbaar: de hoofdlijnen van het Nederlandse politieke systeem zullen niet ingrijpend veranderen de komende jaren. Nederland is in 2030 nog steeds een monarchie en parlementaire democratie met een meerpartijenstelsel. Verder kent Nederland nog steeds drie bestuurslagen (rijk, provincie en gemeenten). De trend van decentralisatie van beleidsontwikkeling zet zich verder door richting gemeenten. Uitvoering van beleid zal door inzet van ICT daarentegen onderhevig zijn aan processen van concentratie en centralisatie. Deze tendens heeft geleid tot een kleiner overheidsapparaat dat zich vooral bezighoudt met beleidsontwikkeling en handhaving. Steeds minder mensen zijn lid van een politieke partij.
De *Europese eenwording* zal zich op economisch en geografisch gebied doorzetten, met een voortgaande uitbreiding met kandidaat-landen die aan politieke en economische basisvoorwaarden voldoen. De vorming van een Europees gebied van vrije markt, vrijheid en vrede biedt kansen om een grotere plaats en een belangrijkere stem te hebben in de wereld. De economische verwachtingen zijn groot: een markt van 500 miljoen consumenten, ondersteund door een economische en monetaire unie, zal meer gewicht in de schaal leggen op de wereldmarkten en in de organisatie van de wereldeconomie.

economie

Voor de scenario's gaan wij voorts uit van de veronderstelling dat het *economische systeem* in Nederland nog steeds gebaseerd is op de vrije markt. Er zal sprake zijn van een kapitalistisch systeem, waarbij investeringen door de overheid in de publieke sector gangbaar zijn. Hoe de economie zich daarbinnen zal ontwikkelen (groei of stagnatie), wordt opengelaten; dit hangt af van tal van factoren, zoals de ontwikkeling van de Amerikaanse dollar ten opzichte van de euro, de olieprijzen, de groeiende positie van Aziatische landen zoals India en China op de wereldmarkt, de wisselwerking tussen vergrijzing en loon- en socialelastenontwikkeling, en de invloed van de Europese eenwording. Een scenario van economische achteruitgang wordt evenwel niet voorzien.
Niettemin wordt verwacht dat er een zekere economische *tweedeling* in de maatschappij zal ontstaan tussen hoogopgeleiden en laagopgeleiden. Het verschil in inkomen tussen deze twee groepen zal toenemen. Hierdoor ontstaat steeds meer een tweedeling in de maatschappij.[5] Een andersoortige ontwikkeling die mogelijk belangrijker wordt is een geleidelijk scherper wordende tweedeling tussen gezonden

[5] Zie *Four futures of Europe*, CPB 2003.

en zieken, tussen arbeidsgeschikten en arbeidsongeschikten, of wellicht tussen personen met een 'gezond' profiel en personen met een verhoogd 'ziekteprofiel', waarbij risicoprofielen worden samengesteld op basis van een combinatie van kennis over genetische aanleg en kennis van levensstijlen. Dergelijke risicoprofielen zullen een toenemende rol kunnen spelen in beslissingen over deelname aan het arbeidsproces, levens- arbeidsongeschiktheidsverzekeringen en pensioenvoorzieningen.
Andere maatschappelijke ontwikkelingen zijn de flexibilisering van *werkpatronen*. Deze tendens is enerzijds gevoed door het feit dat iedereen continu online is en altijd en overal kan werken.[6] Anderzijds is telewerken noodzakelijk geworden doordat de mobiliteit omwille van teruglopende voorraden fossiele brandstoffen noodzakelijk is beperkt.[7] Zowel werktijden als werkplaatsen zijn volledig flexibel geworden. Er is veel sterker dan nu het geval is sprake van een dienstenmaatschappij, waarbij het aantal personen werkzaam in zelfstandige beroepen aanmerkelijk is vergroot.
De *communicatiebehoefte* tussen individuen neemt toe, mede als gevolg van de afname van de mobiliteit halverwege het tweede decennium. Er vindt een sterke convergentie plaats van functionaliteit in mobiele ICT-apparatuur waardoor de communicatie door middel van deze apparatuur als goed substituut geldt voor traditioneel contact. Tegelijkertijd is de MTV-generatie in 2030 volwassen geworden; dit betekent dat de wijze van interactie van mensen met de omgeving verandert. De concentratieperiode van mensen is in 2030 (nog) korter dan in 2004, en de aard van prikkels waarop mensen (kunnen) reageren is anders; MTV en televisiereclames zijn wat betreft vorm de maatstaf, en vrijwel iedereen kan met de snelheid van deze communicatie overweg. De aandacht van mensen is over meer zaken tegelijk verspreid, multitasking neemt dus verder toe. Daartegenover staat een significante groep ouderen, zie hieronder, die niet goed overweg kan met dit bombardement op de zintuigen.

demografie

Op *demografisch vlak* zien we een kleine toename van de bevolkingsgroei voor de komende jaren. Meer mensen, met name autochtonen, verlaten Nederland, waardoor ook het aantal geboorten afneemt. Immigratie en verlengde levensduur zorgen echter nog wel voor een beperkte groei. Volgens de prognose van het CBS uit december 2004 wordt rond 2035 een bevolkingsomvang bereikt van 17 miljoen inwoners. Volgens het CBS is immigratie van niet-westerse allochtonen de belangrijkste factor in de bevolkingsgroei. Het aandeel niet-westerse allochtonen zal stijgen van 10% nu tot 17% in 2050; ook het aandeel westerse allochtonen stijgt, van 9% nu tot 13% in 2050.[8] Het aantal allochtonen zal vooral ook in de grote steden toenemen; Rotterdam verwacht voor de periode 2002–2017 een toename van het aantal personen binnen aandachtsgroepen van 207.234 (2002) tot 305.090 (2017);[9] Amsterdam verwacht een stijging van het percentage van niet-westerse allochtonen van 38,5 (2003) tot 47,4 (2020).[10]
De *vergrijzing* zal sterk toenemen. Volgens het CBS zal de komende veertig jaar het percentage 65-plussers vrijwel verdubbelen van 14 procent nu tot ongeveer 24 (rond 2040).[11] Een iets afnemende groene druk (minder jongeren) wordt eerst geleidelijk en vanaf 2010 zeer nadrukkelijk teniet gedaan door een oplopende grijze druk (meer ouderen).[12] Dit leidt tot een verhoogde belastingdruk, voor vooral de jonge, werkende generatie, mogelijk leidend tot economische teruggang.[13] Daarbij zal ook het aantal eenpersoonshuishoudens, onder andere van alleenstaande ouderen, toenemen. Een

[6] Zie bijvoorbeeld het onderzoek van TNO Arbeid naar virtualisering van organisaties uit december 2004: 'Virtualisering leidt tot werken op afstand: een medewerker, team of organisatie kan onafhankelijk van plaats of tijd aan de slag gaan en afstemmen met klanten, collega's, teams of andere organisaties.' <http://www.arbeid.tno.nl/nieuws/20041222.html>.
[7] Zie onder meer Vraaggesprek Erik Huizer.
[8] <http://www.overheidsinformatie.nl/default.asp?orgidt=Org_016220>.
[9] Volgens het Rotterdamse Centrum Voor Onderzoek en Statistiek (COS).
[10] Volgens het Amsterdamse bureau Onderzoek en Statistiek (O&S).
[11] <http://www.overheidsinformatie.nl/default.asp?orgidt=Org_016220>.
[12] NIDI-rapport, Demos 1997.
[13] *Four futures of Europe*, CPB 2003.

radicalere visie op vergrijzing wordt geboden door wetenschappers die meer nadruk leggen op de rol van medische techniek in het verhogen van de leeftijdsverwachting en/of de kwaliteit van leven. Fukuyama schetst een toekomstbeeld waarin mensen steeds ouder worden doordat stamcelonderzoek het mogelijk maakt om cellen te verjongen en daardoor het natuurlijke verouderingsproces kan worden tegengegaan.[14] De leeftijdspyramide verandert daardoor drastisch: in Europa en Japan wordt een mediaan van leeftijd verwacht rond de 60 (vergelijk: in Derde Wereld blijft die rond de 20). (De mediaan is het getal waarbij aan weerszijden evenveel aantallen bestaan; een mediaan van 60 betekent dat er evenveel 60-plussers als 60-minners zijn.)[15]

2.2. Maatschappelijke variabelen

Binnen de geschetste context van maatschappelijke ontwikkelingen, lichten wij twee maatschappelijke aspecten uit die direct relevant zijn in het licht van de mogelijke ontwikkeling van een veiligheidsmaatschappij c.q. een privacymaatschappij. Deze twee aspecten hanteren wij als variabelen die we uiteenlopend invullen voor de beide scenario's.

Variabele 1: de rol van de overheid

Het type rol dat de overheid inneemt is van fundamenteel belang in elk toekomstscenario. Hierbij zijn diverse keuzes denkbaar, die elk met goed recht verdedigd kunnen worden. Wij hebben ervoor gekozen om bij het veiligheidsscenario een terugtredende overheid te schetsen, vanuit het idee om de "rechtse" thema's van veiligheid en een slanke overheid-op-afstand te koppelen. Een sterk optredende overheid in een veiligheidsscenario is ook denkbaar, maar wij achten een politiestaat iets minder realistisch dan een nachtwakerstaat. Bij het privacyscenario kiezen wij, om vergelijkbare redenen, voor een optredende overheid, door de koppeling van de "linkse" thema's van privacy en een actieve, beschermende overheid.

veiligheid

In het *veiligheidsscenario* van 2030 zal de Nederlandse overheid aldus voornamelijk fungeren als een nachtwakerstaat: zij heeft zich dan teruggetrokken op een beperkt aantal, beschermende functies. De handhaving van orde en gezag is de belangrijkste taak van de overheid, met een nadruk op de veiligheid van grote maatschappelijke instituties, zoals de integriteit van de economie, de nationale veiligheid, vitale infrastructuren en internationale betrekkingen. In het algemeen zal de Nederlandse overheid zich zeer terughoudend opstellen: waar mogelijk worden activiteiten aan de markt overgelaten.

Collectieve veiligheid is daarmee een van de belangrijkste terreinen van overheidsbemoeienis geworden. Vanuit dat belang heeft de Nederlandse overheid dan ook vergaande bevoegdheden en middelen tot haar beschikking. Daartoe werkt zij nauw samen met de talloze particuliere beveiligingsorganisaties in Nederland, die ten behoeve van de individuele veiligheid van Nederlanders commerciële diensten aanbieden. Ook zijn er allerhande samenwerkingsverbanden met publieke en private beveiligingsorganisaties over de landsgrenzen heen. Privacybescherming wordt beschouwd als een individueel goed dat niet onder de verantwoordelijkheid van de Nederlandse overheid valt, maar via marktregulering voor Nederlandse burgers 'te koop' is.

In deze Nederlandse nachtwakerstaat van 2030 heeft de overheid zich teruggetrokken op haar kerntaken en zoveel mogelijk activiteiten aan de markt en de samenleving overgelaten: veiligheid en privacy worden toenemend geprivatiseerd en gecommercialiseerd. Burgers zijn grotendeels aangewezen op eigen initiatief om aan

[14] Vergelijk de ontdekking van een genvariant in het SHC1-gen die het verouderingsproces lijkt te remmen: S.P. Mooijaart e.a., 'Variation in the SHC1 gene and longevity in humans', *Experimental Gerontology* februari 2004, samenvatting in <http://www.leidenuniv.nl/mare/2004/24/0702.html>; alsmede het gerapporteerde stoppen van veroudering in wormen: 'Tweaking Genes and Hormones Gives Worms Lifespan of 500 Human Years', 24 October 2003, beschikbaar via <http://www.betterhumans.com/>.

[15] Fukuyama 2002, p. 9 en p. 62-3.

hun individuele behoeften ten aanzien van veiligheid en privacy zoveel mogelijk tegemoet te komen. Mogelijkheden voor eigen initiatief worden in belangrijke mate bepaald door het inkomen waarover burgers beschikken. Deze situatie brengt een ontwikkeling van sociaal-economische groepsvorming met zich mee die uitmondt in de totstandkoming van woonwijken met bewoners die allen tot een specifieke sociaal-economische laag van de bevolking behoren en zich een zekere mate van veiligheid en privacybescherming financieel kunnen veroorloven. De markt zal op deze ontwikkelingen inspelen, wat zal leiden tot een verdere privatisering en commercialisering van dienstverlening op het gebied van veiligheid en privacybescherming. Naarmate het gemiddelde inkomen in een wijk hoger is, zullen de wijkbewoners derhalve meer maatregelen kunnen treffen om aan hun behoeften van veiligheid en privacy tegemoet te komen. Zo kunnen zij bijvoorbeeld ervoor kiezen om particuliere beveiligingsorganisaties in te huren, beveiligingsinstallaties aan te schaffen, hekwerken om hun perceel en/of om hun wijk heen aan te brengen en individueel of collectief cameratoezicht te organiseren.
Omdat de overheid ook de privacybescherming allengs meer aan het privé-initiatief overlaat, zullen rijke mensen in 2030 beter in staat zijn om hun privacy te beschermen dan arme. De rijken zullen met name gebruik maken van de traditionele dienstverlening van private bewakings- en beveiliginsorganisaties om hun ruimtelijke, fysieke en relationele privacy te beschermen. De grote groepen aan de onderkant van de samenleving zullen zich dit niet kunnen permitteren. Voor wat betreft de informationele privacy ligt dit ingewikkelder. Omdat mensen zoveel directe belangen hebben bij de integratie van computers, sensoren en netwerken in hun leef-omgeving, zullen zij snel bereid zijn het gebruik en hergebruik van hun persoonsgegevens toe te staan. Men zal echter willen optreden tegen concrete consequenties van bepaalde toepassingen, zoals het openbaar maken van informatie die kan leiden tot een inbreuk op de ruimtelijke, fysieke of relationele privacy. Hieroe zal men algemene wetgeving of aanpassing daarvan verlangen.

privacy

In het *privacyscenario* van 2030 zal de Nederlandse overheid zich manifesteren als een actieve, beschermende overheid. Een groot aantal beschermende, ordenende, stimulerende en ontwikkelende functies behoren dan tot haar activiteitengebied, dat gericht is op optimale welvaarts- en welzijnsverhoudingen voor alle in Nederland wonende personen. De sterke staatsbemoeienis komt vooral tot uiting in het beschermen, stimuleren en ontwikkelen van kwetsbare doelgroepen in de Nederlandse samenleving. Veel staatsinspanningen zijn derhalve gericht op het dusdanig faciliteren van het individuele voorzieningenniveau van burgers, dat elke burger in Nederland op een zeer redelijk welzijnsniveau kan leven. Individuele privacybescherming voor elke inwoner van Nederland is daarmee een belangrijke collectieve verantwoordelijkheid van de Nederlandse overheid: privacybescherming via marktwerking zou immers vanuit een overheidsoptiek onacceptabele verschillen tussen burgers teweeg brengen. De Nederlandse overheid zal dan ook waar mogelijk optreden om daarmee de verschillen in privacybescherming tegen te gaan die door marktwerking worden gegenereerd. Voorbeelden van overheidsactiviteiten die in het belang van individuele privacybescherming kunnen worden uitgeoefend door de optredende overheid van 2030, zijn uitgebreide onderwijs- en trainingsfaciliteiten, het via regelgeving afdwingen van het gebruik van PETs (*Privacy-Enhancing Technologies*) in de Nederlandse samenleving, en het stimuleren en faciliteren van volkshuisvesting waarbij zoveel mogelijk rekening wordt gehouden met privacybehoeften van individuele bewoners.
Privatisering en commercialisering van veiligheid en privacy zullen bij de optredende overheid wel aanwezig zijn: ook in dit scenario zal beveiliging meer dan in 2005 voorwerp zijn van private initiatieven en publiek-private samenwerking. Deze private initiatieven zullen echter aan strenge regels en toezicht gebonden zijn (zie ook par. 4.1). Privacybescherming zal evenwel minder worden geprivatiseerd: de overheid rekent het nog steeds tot haar taak om de privacy van alle burgers te beschermen.

Door het opgaan van computers, sensoren en netwerken in de directe leef- en werkomgeving van de burgers, is dat er evenwel niet gemakkelijker op geworden.

Variabele 2: de mate van discriminatie
Mede door de verschillende de rol van de overheid en de mate waarin private verantwoordelijkheden de norm worden in de maatschappij, zal ook de mate van discriminatie tussen bevolkingsgroepen uiteen kunnen lopen.

veiligheid

In het *veiligheidsscenario* zal een terugtredende overheid meer nadruk leggen op bescherming van grootschalige instituties als de economie en de beveiliging van grote infrastructuren, en minder nadruk op de bescherming van kwetsbare groepen. Hierdoor zal de tweedeling tussen hogeropgeleiden en laagopgeleiden scherper tot uitdrukking komen in de maatschappij dan in het privacyscenario het geval is. Omdat ook de sectoren van onderwijs en gezondheidszorg een privatiseringstendens hebben doorgemaakt (voor goed onderwijs en goede zorg moet de burger zelf meer gaan betalen), is de sociale mobiliteit afgenomen. De relatief rijke bovenklasse wordt juist – letterlijk – gekenmerkt door een grote mate van mobiliteit. Het gaat om een groep van goed opgeleide, gezonde Europeanen die zich gemakkelijk over het Europese grondgebied bewegen, op zoek naar werk en kansen op gewin. Zij zullen eisen dat de veiligheid bij deze mobiliteit wordt gewaarborgd, door nadruk op zware bescherming van de transportsector en de openbare ruimte. Dat gaat gepaard met beveiligingsmaatregelen die enige discriminatie in de hand werken: de hoogopgeleiden kopen de beveiligingsmaatregelen af met technische hoogstandjes die hen in staat stellen soepel langs alle controles te gaan; de diverse groepen laagopgeleiden zullen zich vaker dan de hoogopgeleiden moeten identificeren, legitimeren en verantwoorden wanneer zij zich – binnen hun beperktere mogelijkheden – begeven in de openbare ruimte. Door het ontstaan van hekwerkwijken (*gated communities*) is de openbare ruimte bovendien beperkt. De leefwereld van de sociaal-economisch zwakkeren is daarbovenop nog beperkt doordat de fysieke mobiliteit voor deze groep door de toegenomen energiekosten en het ontbreken van alternatieven afneemt. De daaruit voortvloeiende gevoelens van onvrede leiden tot tegenstellingen tussen de diverse bevolkingsgroepen die groter zijn dan in de huidige maatschappij.

privacy

In het *privacyscenario* zal de bescherming van zwakke groepen en de erkenning van privacybehoeften ertoe leiden dat veiligheidsmaatregelen 'eerlijk' worden toegepast. Veiligheidscontroles in de transportsector en op straat zullen niet erg scherp zijn, waardoor er geen dure 'ontheffingstechnieken' ingekocht hoeven te worden en waardoor ook de laagopgeleiden zich vrijer weten te bewegen. De met privacywaarborgen omklede controles op straat leiden echter tot enkele prominente incidenten waarbij misdadigers niet tijdig gesignaleerd zijn en daardoor hebben kunnen ontkomen. Aangezien bij de meerderheid van die incidenten burgers uit onderklassen betrokken zijn, neemt de spanning tussen verschillende segmenten in de maatschappij toe. Enerzijds is er een maatschappelijke druk om bepaalde groepen die worden geassocieerd met deze segmenten aan zwaardere veiligheidsmaatregelen te onderwerpen, die anderzijds door de overheid wordt tegengehouden. Dit spanningsveld uit zich in langdurige, gepolariseerde discussies en compromiswetgeving op vele terreinen van het maatschappelijk verkeer, zoals arbeidsrecht, verzekeringsrecht en gezondheidsrecht, met veelal als uitkomst non-discriminatoire regelgeving die in de praktijk niet altijd non-discriminatoir kan worden toegepast.

3. Techniek

Techniek ontwikkelt zich snel – en, in elk geval vooralsnog, steeds sneller. Wie de voortschrijding in techniek bestudeert per decennium, zal opvallen dat de sprongen in technische ontwikkeling steeds dichter op elkaar zitten, mede doordat vakgebieden in elkaar overvloeien, waardoor kennis uit aanpalende vakgebieden

plotseling geïncorporeerd kan worden. Er lijkt soms zelfs sprake van een exponentiële ontwikkeling in kennis en techniek. Wij gaan in deze studie uit van een voortzetting van deze versnellingstendens, zodat de extrapolatie van huidige technische ontwikkelingen grotere sprongen vertoont dan de andere contexten die wij beschrijven. Op de lezer die niet geheel is ingevoerd in de nieuwste stand van zaken op een bepaald technologiegebied, zullen de scenario's soms ook als *science fiction* overkomen. Dat is ook onze opzet: voor een technisch toekomstscenario geldt: 'If it doesn't sound like science fiction, then it's probably wrong.'[16]

3.1. Technische context en ontwikkelingen

ICT (in ruime zin)

data mining

Datamining-technieken zullen een grote vlucht nemen. Door middel van kunstmatige-intelligentietechnieken wordt het steeds beter mogelijk om 'vervuilde' bestanden aan elkaar te koppelen en problemen die ontstaan door verschillende gegevensdefinities in bestanden op te lossen. Deze ontwikkeling wordt voor een belangrijk deel vanuit de commerciële sector gestuurd, waarbij de overheid overigens gretig aanhaakt. Er vindt een sterke consolidatie plaats van aanbieders van informatie die behoefte hebben aan een gedegen inzicht in hun klanten. Advertentieaanbieders, zoals DoubleClick, spelen een centrale rol in dezen. Zij bieden hun reclames aan op duizenden webpagina's en verkrijgen hierdoor inzicht in het surfgedrag van mensen – een inzicht dat ruim uitstijgt boven dat van hun klanten.[17]

Alle ICT is mobiel, en de *mobiele apparatuur* is uitgerust met hogeresolutiebeeldschermen, camera's en locatiebepaling, en in de wat verdere toekomst ook met tactiele en wellicht ook olfactorische gegevensoverdracht (zie hieronder, *virtual reality*); de apparaten zijn in staat om spraak in tekst om te zetten, en omgekeerd. Chatten en sms'en zijn centrale vormen van communicatie, zij het dat de wijze waarop dit plaats vindt door techologische vooruitgang verandert. Wat niet verandert is het staccato- en betrekkelijk vluchtige karakter van deze vorm van communicatie.

ambient intelligence

Ambient Intelligence zal in 2030 gemeengoed zijn. Dit is een concept waarin de informatiesamenleving zodanig ingericht is dat individuen in hun dagelijks leven worden omgeven door een breed scala aan intelligente en intuïtieve technologie die is ingebed in een diversiteit aan objecten die ons in het dagelijks leven omringen. Deze 'intelligente' omgeving zal dan in staat zijn gedrag van mensen te herkennen, daarop te reageren en ook te anticiperen. Gebruiksvriendelijkheid, efficiënte ondersteuning van menselijk handelen en *user-empowerment* zijn verwachte voordelen van het concept. Met behulp van AI-technologie kan een grootschalig, op technologie gebaseerd collectief sociaal geheugen worden gerealiseerd, dat individuen in staat stelt direct commentaar en reacties te krijgen op hun (sociale) handelen. Daarmee ontstaat een door intelligente en intuïtieve technologie ondersteund 'social learning process'.[18] Een dergelijk gedigitaliseerd collectief geheugen biedt, in combinatie met de sturingsmogelijkheden van de techniek, vele nieuwe mogelijkheden om mensen te controleren, hun gedrag te beïnvloeden en daarop te anticiperen. Dit creëert enerzijds belangwekkende nieuwe mogelijkheden voor opsporing en handhaving en daarmee het optimaliseren van veiligheid: de intelligente omgeving kan immers alle gedragingen van mensen onthouden en langdurig opslaan. Bovendien kan geanticipeerd worden op mogelijk riskant gedrag, waarbij agressiedetectiesystemen (zie onder) een waarschuwingssignaal doen afgaan. Tegelijkertijd ontstaan daarmee ook risico's van manipulatie en controle: de omgeving zal meer dan voorheen invloed hebben op het gedrag van mensen en dat gedrag in toenemende mate kunnen sturen. Het individu loopt dan het risico gestuurd en beheerst te worden door zijn omgeving.[19] Vanuit privacyperspectief treedt dan de

[16] Chris Peterson, geciteerd in Mulhall 2002, p. 21.
[17] Zie ook Vraaggesprek Erik Huizer.
[18] ISTAG 2001.
[19] Zie ook Vraaggesprek Ulco van de Pol.

vraag naar voren welke beschermingsinstrumenten noodzakelijk zijn tegen een te verregaande allesomvattende (her)kenbaarheid en stuurbaarheid van mensen en hun handelen. Te verwachten valt in elk geval dat in bepaalde domeinen, zoals het verkeer en in winkels, *ambient intelligence* volop gebruikt zal worden niet alleen voor het comfort maar ook voor de sturing van individuen, met als argument het voorkomen van ongevallen en misdrijven.

virtual reality Een gerelateerde ontwikkeling is *virtual reality*, waardoor langzamerhand – en in beperkte mate – fysieke contacten tussen mensen afnemen. Het contact leggen met anderen kan immers ook in de virtuele wereld plaatsvinden, wanneer zowel personen als hun woonomgeving altijd online en direct waarneembaar zijn. De advertentiecampagne die eind 2004 de burgers aanmoedigt om mobiele telefonie te gebruiken waarbij je elkaar kunt zien wanneer je belt, is een voorproefje van de mogelijkheden die *virtual reality* biedt: niet alleen geluid en beeld, maar ook tastzin en reuk kunnen in beginsel op afstand worden overgedragen in steeds laagdrempeliger toepassingen. In 2030 is het technisch mogelijk een ultralichte handschoen bij je te dragen waarmee je bij een telefoongesprek iemand voelbaar de hand kunt schudden. 'Telefoongesprek' is dan ook een verouderde term: men zal veeleer een tele-ontmoeting hebben, waarbij gevoelsmatig de nadruk meer op ontmoeting en minder op tele ligt. Verbonden zijn met anderen, inclusief lichamelijk contact, vindt aldus vaker plaats via technologie, en de ontmoeting in fysieke nabijheid raakt gaandeweg wat op de achtergrond. Toch zal ook de nodige behoefte blijven bestaan aan 'the real thing': virtuele werkelijkheden zullen niet volledig de fysieke werkelijkheid verdringen, en fysiek transport en fysieke werkruimtes blijven dan ook belangrijke onderdelen van de maatschappij van 2030.

localisering *Locatietechnologie* neemt een grote vlucht. Aan de ene kant valt waar te nemen dat mobiele apparatuur, zoals camera's, uitgerust worden met GPS-ontvangers zodat de locatie waar een bepaalde foto is gemaakt als metadata aan de foto kan worden toegevoegd. De computer waarop de foto's worden uitgelezen is dan in staat aan te geven waar de foto is gemaakt. De vraag "waar was deze fantastisch besneeuwde berg ook maar weer?" behoort hierdoor tot het verleden. Anderzijds neemt celgebaseerde communicatie (GSM, GPRS, WiFi, WiMax) een grote vlucht. Deze technologie maakt locatiebepaling van de gebruikte apparatuur inherent mogelijk. In hoeverre celtechnologie zich ontwikkelt naast vaste breedbandverbindingen is mede afhankelijk van het overheidsbeleid ten aanzien van communicatiebanden in de ether.[20] Overigens is locatiebepaling op het vaste net eveneens mogelijk. In samenhang met de toenemende vastlegging van (verkeers)gegevens, betekent dit dat de locatie van eenieder die zich van ICT-(communicatie)apparatuur bedient in beginsel altijd beschikbaar is. De nauwkeurigheid van die locatiebepaling hangt af van de gebruikte technologie. Deze locatiegegevens zullen worden gebruikt voor de reeds bestaande doelen: facturering, opsporing en vervolging, en nationaleveiligheidsbescherming. Daarnaast zal het gebruik van locatiebepaling voor plaatsgerelateerde mobiele diensten sterk toenemen: de mobiele burger zal overal informatie ontvangen die afhangt van zijn locatie. Reclameberichten zullen bijvoorbeeld aan de passant van een winkel worden gestuurd wanneer deze binnen de doelgroep van de winkel valt.[21] Ook in het geval van rampen of ander gevaar zullen de locatiegegevens worden gebruikt om de betrokkenen gericht te waarschuwen via berichten aan allen die zich in een getroffen gebied bevinden. Ieder mobiel apparaat bevat bovendien een verplichte *panic button* die een hulpsignaal en de locatie van de gebruiker doorgeeft aan hulpinstanties.

[20] Een belangrijk deel van de RF-banden (Radio Frequency) is voorbehouden voor militaire communicatie. Dit beperkt de mogelijkheden voor draadloze breedbandtoepassingen aanzienlijk. Zie ook het vraaggesprek met Erik Huizer.

[21] Zie de persoonlijke aansporing die het personage John Anderton (Tom Cruise) in Minority Report met naam en toenaam krijgt om de spanningen van zich af te werpen door het nuttigen van een Guinness in een bar waar hij langsloopt.

Biotechnologie

biotech Biotechnologie zal zich substantieel verder ontwikkelen en de nodige toepassingen bieden die nu nog moeilijk voorstelbaar zijn. Voor de scenario's laten wij ontwikkelingen op het gebied van klonen en genetische gemodificeerde organismen (voedsel-genomics) buiten beschouwing; deze zijn niet wezenlijk voor de privacy en de veiligheid die in deze studie centraal staan. Ontwikkelingen in DNA-technologie en -kennis, alsmede toepassingen op gerelateerde gebied van eiwitten (proteomics) en neurofarmacologie komen in par. 3.2 aan bod.

Nanotechnologie[22]

slimme materialen Op het gebied van de nanotechnologie worden steeds meer 'slimme' toepassingen ontwikkeld. Een voorbeeld daarvan is de 'slimme' bumper die binnen afzienbare tijd wellicht technisch haalbaar zal worden. Bij een botsing deukt deze bumper automatisch mee (en weer terug) zodat minder letsel wordt veroorzaakt. Op lange termijn worden ook lichte auto's verhoopt die een dermate flexibel maar robuust gestel hebben dat bij botsingen en over-de-kop-slaan de auto rekbaarder is en – als een stuiterbal – terugveert.[23]
Een andere toepassing van nanotechnologie die op middellange termijn (grofweg over 10 tot 20 jaar) wordt verwacht, is slimme kleding. Soldatenpakken zitten bijvoorbeeld vol met nanosensoren en elektronica waardoor de soldaat meer en meer beschermd wordt tegen de gevaren van het slagveld. De nieuwe pakken zijn in staat om door middel van energieabsorberende materialen een ontploffingsgolf te weerstaan, ondoordringbaar ineen te krimpen in geval van bio-aanvallen, en met behulp van sensoren (bloed)wonden te kunnen signaleren en indien nodig te stelpen. Bovendien krijgt kleding kameleontische eigenschappen: door de specifieke eigenschappen van nanodeeltjes waaruit textiel wordt opgebouwd, zal kleding van kleur kunnen veranderen om zich aan te passen aan de omgeving.[24] Dezelfde toepassing zal mogelijk worden in tal van verfoppervlakken, zodat auto's, tassen en andere accessoires op afroep een andere kleur kunnen krijgen. Dit heeft mede tot gevolg dat verklaringen van getuigen, die voor een groot deel gebaseerd zijn op kledings- en kleurkenmerken, (nog) minder betrouwbaar worden.

nanobots Op lange termijn – 2030 is daarvoor aan de vroege kant – kan men ook denken aan nanorobotjes. In 1986 reeds introduceerde Eric Drexler in zijn boek *Engines of Creation* de mogelijkheid van ultrakleine robotjes die in staat zouden zijn om zichzelf te verplaatsen, organiseren en repliceren. Dergelijke nanodeeltjes zouden bijvoorbeeld schade aan het milieu ongedaan kunnen maken (door olie op zee af te breken), en ziekten kunnen genezen of voorkomen door bijvoorbeeld in het menselijk lichaam vroegtijdig kankercellen op te sporen.[25] Of dergelijke toepassingen ooit mogelijk worden, wordt overigens betwijfeld door de nodige wetenschappers.[26]

---

[22] Nanotechnologie is gericht op het maken van systemen op een schaal van 1 tot 100 nanometer (1 nm = één miljardste meter). Deze systemen worden opgebouwd uit individuele atomen, en kunnen bijvoorbeeld worden ingezet in kunstmaterialen en in biotechnologische toepassingen binnen het lichaam.

[23] "Embedded into a composite, NTs [nanotechnologies] have enormous resilience and tensile strength, and could be used to make cars that bounce in a wreck or buildings that sway rather than crack in an earthquake." Collins & Avouris 2000.

[24] "Living materials are capable of doing things such as self-healing, or being able to reconfigure their overall structure, color, or properties, based on the cells' physiology and the cells' needs, as opposed to synthetic materials, which are just static in nature," says Bachand. "Once you form them, there they are, and that's pretty much what you're going to get. What we're trying to mimic is the ability of some living organisms" – including some fish and other marine creatures such as octopi and squid – "to change color in response to changing light conditions", geciteerd in Karen Lurie, 'Quick-Change Stuff', ScienCentralNews 10 February 2003, <http://www.sciencentral.com/articles/view.php3?language=english&type=article&article_id=218392073>. 'Zudem könnten Verbesserungen beim (...) indirekten Schutz militärischer Fahrzeuge (Tarnen und Täuschen, z.B. durch Farbwechsel mit "intelligenten" Oberflächenbeschichtungen) erreicht werden.' TAB 2003.

[25] 'Indeed, nanorobots may be designed to read from, and write to, the stored information in a cell's genetic code to check for errors and viruses, and to repair damage resulting from age, radiation, or toxic chemicals. The potential of such a technology is staggering, and it is not too early to begin thinking about the problems -- and opportunities -- it may create.' Fiedler & Reynolds 1994, p. 625.

[26] Een gezamenlijke werkgroep van de Britse Royal Society & Royal Academy of Engineering (2004) concludeert bijvoorbeeld dat er geen bewijs is voor uitspraken dat nanotechnologie daadwerkelijk op de korte en middellange

Niettemin is voor de toekomst van veiligheid zeker relevant de mogelijke ontwikkeling van onzichtbare deeltjes (of die nu op nano- of op microschaal werken) die een zekere mate van zelfstandigheid hebben. Nanobotjes (of microbotjes) zouden, al dan niet in combinatie met biologische virussen of ingeprogrammeerde kenmerken van dergelijke virussen, wellicht in enige vorm ingezet kunnen worden bij een terroristische of oorlogsaanval.[27] Een veiligheidsmaatschappij zal daarom de nodige aandacht moeten besteden aan de gecontroleerde ontwikkeling van nanotechnologie,[28] en door middel van *technology assessment* ook vroegtijdig de risico's van kwalijke toepassingen van nanodeeltjes moeten inschatten.

Robotica

robots

Het gebruik van robots neemt snel toe, niet alleen in industriële toepassingen, maar vooral ook in het dagelijkse leven. Daarbij moet men niet zozeer denken aan tweebenige, twee-ogige en twee-antennige robots die we kennen uit *science-fiction*films, maar aan functionele apparaten die zelfstandig taken verrichten. Anno 2004 kennen we al grasmaairobots, stofzuigrobots en strijkrobots, maar ook gezelschapsrobots als de Aibo.[29] In 2030 zullen dergelijke robots gemeengoed zijn en onopvallend onderdeel zijn van de huishouding. Of het robotvoetbalelftal dan al zal winnen van het menselijk wereldelftal is een open vraag, maar evenals bij schaken is gebeurd, valt te verwachten dat ooit het robotelftal sterker zal blijken.[30] De belangrijkste vraag is tot hoever de 'autonomisering' van robots zal gaan. Deze zal zeker doorzetten en het lijkt zeer waarschijnlijk dat in 2030 multifunctionele robots zelfstandig de straat op gaan en in de publieke ruimte taken vervullen.[31] Daarnaast zullen robots ook meer zichzelf opbouwen en repareren.[32] Maar wij verwachten dat de autonomisering niet onbeperkt doorgaat: evenals bij nanotechnologie[33] zal men vroeg genoeg de gevaren van zichzelf reproducerende en zelfstandig loslopende robots erkennen, en functionaliteiten inbouwen die de autonomie binnen de menselijke perken houden (door een – draadloos bedienbare – aan/uit-knop die mensen wel maar robots niet zullen kunnen bedienen). Ook zullen robots aan vergelijkbare veiligheidsmaatregelen worden onderworpen als burgers, zoals een identificatieplicht.[34] Wij sluiten ons dus niet aan bij het toekomstscenario van Mulhall van een *Robo sapiens* die rechten zal opeisen en de mensheid dreigt te gaan verdringen.[35] Incidentele ongelukken daargelaten, zullen robots eerder in de maatschappij van 2030 een nuttige rol vervullen die bijdraagt aan het gemak van de mens. Dat gemak zal wel ten koste kunnen gaan van de keuzevrijheid van de burger,

---

termijn kan helpen kanker de wereld uit te helpen. Dergelijke stellingen getuigen volgens de werkgroep eerder van een naïef beeld van de opsporing en bestrijding van kankercellen.

[27] 'More advanced applications, however, are likely to be both powerful and subtle: devices that can infiltrate electronics and seize control at crucial moments, artificial "disease" agents that can rest harmlessly in victim's bodies until activated by an external signal, (...) nanotechnology-based agents for crop destruction, forest-cover removal'. Reynolds 2001.

[28] Vergelijk The Foresight Guidelines die zijn opgesteld om de ontwikkeling van nanotechnologie onder controle te houden; opgenomen in Reynolds 2001.

[29] Een recent VN-rapport geeft aan dat er momenteel 607.000 huishoudelijke robots zijn, waarvan 65% het afgelopen jaar werd gekocht. In 2007 verwacht de VN 4,1 miljoen huishoudrobots wereldwijd, die bijvoorbeeld zwembaden schoonmaken en de ramen lappen, maar er zullen ook 2,5 miljoen 'vrijetijdsrobots' zijn. Aldus *NRC Handelsblad* 23 oktober 2004. Zie voor de aaibare Aibo: <http://www.sony.net/Products/aibo/index.html>.

[30] Zie <http://www.fira.net>.

[31] Reeds in 2003 heeft Honda dergelijke robots geproduceerd: 'Asimo kan onder meer mensen begroeten, gezichten herkennen en reageren op zijn omgeving. Honda heeft een twintigtal Asimo's geproduceerd, waarvan er enkele werkzaam zijn als museumgids en als receptionist', Automatisering Gids 18 juli 2003, geciteerd in Stuurman 2003, p. 213.

[32] Een Deense universiteit heeft samen met Lego de Hydra ontwikkeld, een robot die zichzelf in de juiste vorm kan brengen. 'De zelfgroeiende robots assembleren zichzelf zonder menselijke tussenkomst. Omdat ze uit uniforme bouwstenen zijn samengesteld is reparatie heel eenvoudig door het uitwisselen van defecte modules.' *Automatisering Gids* 19 november 2004.

[33] Zie The Foresight Guidelines, noot 28.

[34] 'Hoewel de angst voor groepjes 'rondhangende robots' (een belangrijke reden voor de komende invoering van identificatieplicht voor 14+-ers) overdreven lijkt, kan een verplichting tot identificatie van robots ('robotkentekens') nuttig zijn bij transacties of schadevoorvallen waar robots bij betrokken zijn.' Stuurman 2003, p. 213.

[35] '*Robo sapiens*' are built. This is the first autonomous robot generation with intelligence that rivals that of humans. They begin to replicate themselves (...). Robo sapiens start to ask for rights. Religious terrorists assassinate some, but fail to wipe them out. (...) The antivivisection movement changes its focus to robot rights.' Mulhall 2002, p. 85.

die voor zijn robotgestuurde comfort of veiligheid zich zal moeten laten leiden door de techniek[36] – bijvoorbeeld door volledig geautomatiseerd autoverkeer.

3.2. Technische variabelen

Binnen de geschetste context lichten wij vier technische ontwikkelingen uit wij het meest relevant vinden voor scenario's voor een veiligheidsmaatschappij c.q. een privacymaatschappij. Deze hanteren wij als variabelen die we uiteenlopend invullen voor de beide scenario's.

Variabele 3: verplichte opslag van gegevens

veiligheid De eerste variabele betreft het bewaren van gegevens. In een *veiligheidsscenario* is er sprake van veel wettelijk verplichte opslag van gegevens bij bedrijven en andere private instanties, zoals infotheken, financiële instellingen, winkels, Internet- en telecommunicatieaanbieders, etc. Daarbij gaat het niet langer alleen om het bewaren van persoonsgegevens die samenhangen met een concrete relatie met een individu (zoals gegevens over een verzekering dan wel een aankoop) maar ook om nieuwe gegevens die worden gegenereerd op basis van gecombineerde transactiegegevens. In het veiligheidsscenario zal bovenop de bestaande wettelijk bewaarplichten die voortvloeien uit sectorale wetgeving (Archiefwet, WGBO, BW, etc.) en de dan reeds ingevoerde bewaarplichten voor telecommunicatie-verkeersgegevens, een additioneel wettelijk regime voor de verplichte opslag van in alle mogelijke contexten voorhanden gegevens zijn geïntroduceerd. Te denken valt aan langdurige verplichte opslag van camerabeelden, de inhoud van telecommunicatie, identificatie bij toegang tot gebouwen, maar ook gegevens verkregen uit *datamining*-applicaties en gegevens gegenereerd ten behoeve van gepersonaliseerde dienstverlening door de private en publieke sector. In een dergelijk scenario is bewaren de regel in plaats van uitzondering, in tegenstelling tot het huidige regime van uitsluitend bewaren indien dit (wettelijk) noodzakelijk is. De eisen van subsidiariteit en proportionaliteit worden daarbij ook zeer vrij uitgelegd, en doelbinding is geen wezenlijk criterium.

privacy In een *privacyscenario* zal daarentegen sprake zijn van een restrictief beleid ten aanzien van de verplichte opslag van gegevens door derde instanties. Veel van de opgeslagen gegevens zijn daarbij niet rechtstreeks te herleiden tot individuen, maar alleen door tussenkomst van een vertrouwde tussenpersoon en in beginsel met medeweten van de betrokkene.[37] Wettelijke bewaarplichten zijn primair te vinden in sectorale regelingen en zijn gericht op andere dan politiële en justitiële belangen. Deze bewaarplichten worden slechts zeer spaarzaam aangevuld met bewaarplichten in het belang van veiligheid. Hierbij geldt een zeer strikte interpretatie van de eisen van proportionaliteit, subsidiariteit en doelbinding.

Variabele 4: panoptische technologie

De mogelijkheden tot *surveillance* (in de Engelstalige, brede zin van het woord: het heimelijk in de gaten houden) nemen gestaag toe. Mensen en objecten kunnen gevolgd worden en plaatsen kunnen nauwgezet in de gaten gehouden worden. Naast gebruik van cameratoezicht in de openbare ruimte zal ook het gebruik daarvan in gesloten circuits toenemen: ouders die hun kinderen op het kinderdagverblijf kunnen waarnemen, maar ook kinderen die hun ouders kunnen bewaken in het verzorgingstehuis.[38]

RFID Naast het te verwachten ruime gebruik van cameratoezicht, zal daarbij in belangrijke mate ook gebruik worden gemaakt van Radio Frequency Identification (RFID). Het gebruik van RFID maakt momenteel een snelle opmars, doordat diverse grote afnemers van consumentenproducten het plaatsen van 'tags' op die producten ontwikkelen. Waar aanvankelijk RFID vooral wordt ingezet voor massagoederen (het

[36] Vraaggesprek Ulco van de Pol.
[37] Dit sluit aan bij ontwikkelingen zoals die plaatsvinden binnen het PRIME-project uit het Zesde EU-Kaderprogramma, waarbij PETs voor anoniem en pseudoniem opereren van burgers worden ontwikkeld.
[38] Zie ook Vraaggesprek Erik Huizer.

volgen van containers bijvoorbeeld), zullen in de nabije toekomst individuele producten worden uitgerust met een RFID-chip. Deze 'tags' kunnen op afstand uitgelezen worden door speciaal daarvoor ontwikkelde apparaten. De informatie die op een 'tag' opgeslagen is kan variëren van de kleur, gewicht, productcode en een unieke identificerende code van het product tot de NAW-gegevens van de eigenaar of bezitter van het product.

veiligheid

In het *veiligheidsscenario* worden dergelijke 'panoptische' middelen ingezet om de veiligheid van mensen en plaatsen te garanderen. Cameratoezicht is breed verspreid, in alle publieke en in de meeste semi-publieke ruimten; de beelden worden langere tijd opgeslagen en kunnen naar believen worden gecombineerd met gegevensbanken, zoals pin-transacties, geldopnamen en identificerende toegangscontroles. Bovendien maken de camera's met behulp van gelaatsherkenning koppeling met individuen mogelijk,[39] waarbij ook onverwijld ingrijpen mogelijk is wanneer een gezochte verdachte of loslopende veroordeelde ergens herkend wordt. De beelden zijn in beheer bij een breed scala aan partijen, maar kennen een toegangsmogelijkheid door een centrale beveiligingsinstantie die naar believen een bepaalde camera kan aanroepen, en naar wie meldingen worden gestuurd van gesignaleerde gezochte personen. Vrijwel alle producten en dieren zijn ter voorkoming van diefstal of verlies uitgerust met uniek identificeerbare RFID-chips. Ook kwetsbare mensen, zoals kinderen, dementerende ouderen en zwakzinnigen zijn uitgerust met een chip die hen makkelijk laat traceren. Daarnaast zullen vele individuen zich ook vrijwillig laten chippen, niet alleen om ontvoeringen te voorkomen of te beperken en om snel opgespoord te kunnen worden bij rampen, maar vooral om identiteitsfraude tegen te gaan. De chips bieden een extra identiteitscontrole in aanvulling op de reeds met biometrie beveiligde betaalpassen en kredietkaarten. Vermoedelijk zal een deel van de chips ook heimelijk op enige afstand uitleesbaar zijn; dat geldt in elk geval voor chips op luxegoederen, grote geldcoupures, en identiteitsbewijzen.[40] De beschikkingsmacht over de uitleesapparatuur ligt bij de beveiligingsindustrie; daarnaast hebben justitie en ivd's speciale uitleesapparaten voor bepaalde soorten RFID-chips. Ook hackers kunnen veelal de chips uitlezen, maar omdat het over het algemeen weinig privacybedreigende gegevens betreft, wordt dat niet erg gevonden.
Actieve sensoren, dat wil zeggen sensoren die een actief signaal uitzenden zullen eveneens hun weg vinden. Hierbij moet vooral worden gedacht aan microscopische sensoren die (lucht)druk, temperatuur, windsnelheid, geluid, versnelling en dergelijke meten, en die in staat zijn bewerkingen op de data uit te voeren en deze op bepaalde momenten uit te zenden. Het bereik en het minimale formaat van dergelijke sensoren is lastig in te schatten, maar het feit dat in dit verband wordt gesproken van *smart dust* is veelzeggend.[41]

privacy

In het *privacyscenario* wordt cameratoezicht beperkt toegepast, al zal ook in dit scenario in 2030 de reikwijdte hiervan groter zijn dan in 2005. De beelden worden echter niet langer dan een dag bewaard, en de camera's zijn in beheer bij een versnipperde groep instanties, zodat koppeling van beelden aan elkaar en aan andere gegevensbronnen in de praktijk niet goed mogelijk is. Gelaatsherkenning bij cameratoezicht wordt toegepast, maar slechts met een beperkte groep van gevaarlijk geachte personen waarvan de gelaatsscan – gepseudonimiseerd – in een centrale databank is opgeslagen; de omgeving wordt gewaarschuwd wanneer een mogelijk vuurwapengevaarlijke persoon aanwezig is, zonder de identiteit prijs te geven. Door

[39] Het paspoort bevat immers een gelaatsscan, zie noot 40.
[40] In de VS is reeds een paspoort ontwikkeld dat is uitgerust met een tot 20 meter afstand uitleesbare RFID-chip. ACLU, *Naked Data: How The U.S. Ignored International Concerns and Pushed for Radio Chips In Passports Without Security*, ACLU, 2004. Dit biedt de mogelijkheid bij grenscontroles direct identiteitsgegevens uit te lezen, maar ook om bijvoorbeeld op straat heimelijk te controleren wie langsloopt.
[41] Zie onder meer <http://robotics.eecs.berkeley.edu/~pister/SmartDust/>. 'The sensor nodes will be completely autonomous, and quite small. Each node will contain a sensor, electronics, power supply, and communication hardware, all in a cubic millimeter volume! We will demonstrate some sensor nodes which are so small that they float in the air like dust.' <http://www.darpa.mil/mto/mems/summaries/Projects/University_44.html>.

de beperkingen in het systeem worden minder gezochte personen opgespoord en opgepakt dan in het veiligheidsscenario; aan de andere kant worden ook minder 'vals-positieve' treffers gemaakt waarbij onschuldigen voor een gezochte boef worden aangezien, die – tijdelijk maar publiekelijk kenbaar – onterecht gearresteerd en vastgehouden worden.
In dit scenario zijn ook de meeste producten uitgerust met RFID-chips, maar deze worden automatisch uitgeschakeld zodra een product de winkel – betaald en wel – verlaat. Bovendien wordt spaarzaam omgegaan met unieke codes in individuele chips: de meeste 'tags' bevatten alleen productinformatie. Diefstal en namaak van goederen blijven een hardnekkig fenomeen; voor de opsporing daarvan moeten burgers de nodige opsporingsbevoegdheden dulden, waarvan sommige bevolkingsgroepen en gebieden meer last hebben dan andere. In dit scenario wordt technologie ook ingezet ter bescherming tegen panoptische technologie: wie het zich kan veroorloven schaft RFID-blokkers aan die hij op lichaam en om het huis gebruikt om een veilige ruimte om zich heen te hebben waar derden geen zicht op kunnen hebben. Er is daarbij sprake van enige wapenwedloop in de ontwikkeling van anti-RFID-blokkers om volledige onzichtbaarheid tegen te gaan; hierdoor kunnen voornamelijk de betergestelden duurdere blokkers kopen die een hoger niveau van bescherming bieden; minder gegoeden kunnen zich slechts in mindere mate onttrekken aan de steeds terugkerende inzet van opsporingsmethoden door justitie en private veiligheidsdiensten.

Variabele 5: de DNA-databank
Nederland kent sinds vele jaren een forensische DNA-databank, waarin DNA-profielen en DNA-sporenmateriaal ligt opgeslagen.[42] De databank maakt het mogelijk om het DNA-profiel van bij een misdrijf aangetroffen lichaamsmateriaal te vergelijken met bekende profielen van eerder veroordeelde misdadigers. In oktober 2004 zaten ruim 5000 profielen van personen in de databank;[43] de verwachting is dat dit aantal snel zal gaan groeien nu op 16 september 2004 de wet DNA-onderzoek bij veroordeelden werd aangenomen.[44] Deze wet maakt het mogelijk om celmateriaal af te nemen van personen die veroordeeld zijn voor een misdrijf waarop, kort gezegd, tenminste vier jaren gevangenisstraf staat.[45] De enige restrictie die de wet momenteel biedt is dat geen profiel wordt opgenomen van een veroordeelde bij delicten waarbij DNA naar verwachting geen rol zal spelen, zoals meineed en valsheid in geschrifte. Bij de opsporing van dergelijke misdrijven vindt immers ook geen DNA-onderzoek plaats.[46] Maar dat laatste kan gaan veranderen: het is tegenwoordig mogelijk om DNA-sporen te vinden op brieven, sigarettenpeuken, drinkglazen en binnenkanten van handschoenen, en dat maakt het mogelijk dat bij vele soorten misdrijven DNA een rol kan gaan spelen – ook bij bijvoorbeeld dreigbrieven en vervalste waardepapieren. In 2030 zal vermoedelijk bij zeer veel strafbare feiten wel ergens dergelijk sporenmateriaal kunnen worden aangetroffen, al zullen misdadigers blijven proberen verwarring te zaaien door bijvoorbeeld veel haren van anderen rond te strooien.

Vanwege de grote betrouwbaarheid die aan DNA-onderzoek wordt toegekend bij een treffer in de databank, zal de maatschappelijke druk zeker toenemen om de databank uit te breiden. In het Verenigd Koninkrijk worden momenteel niet alleen van veel veroordeelden DNA-profielen opgeslagen, maar ook van personen die ooit

[42] De DNA-profielen zijn 'uittreksels' uit het DNA-materiaal van veroordeelden; dit profiel bestaat uit getallen die afgeleid zijn uit een tiental plaatsen in het niet-coderende DNA, en biedt dus – een sporadische uitzondering daargelaten – geen inzicht in de erfelijke eigenschappen van de persoon. Dit in tegenstelling tot het DNA-sporenmateriaal, waarbij wel het volledige DNA blijft opgeslagen; dit is echter niet herleidbaar tot een bekende persoon maar behoort bij een vooralsnog onopgelost strafbaar feit.
[43] Zie <http://www.dnasporen.nl>.
[44] Stb. 2004, 465.
[45] Dit is ongeacht de strafmaat in het concrete geval. Iemand die een pak melk steelt uit de supermarkt en daarvoor geldboete krijgt opgelegd, kan ook in de databank terechtkomen – op het misdrijf van diefstal staat immers vier jaren gevangenisstraf.
[46] Kamerstukken 2002/03, 28 685, nr. 3, p. 10.

verdacht zijn geweest van enig misdrijf – ongeacht of het misdrijf iets met DNA-opsporing te maken heeft en ongeacht of zij vervolgens vrijgesproken zijn.[47] De nieuwe Nederlandse wet zou een stap op weg kunnen zijn naar een dergelijke grootschalige databank. Het eindpunt van een dergelijke ontwikkeling kan een databank zijn met een profiel van elke Nederlander of ingezetene. Technisch is dat eenvoudig: nu reeds wordt hielprikbloed van elke nieuwgeborene in Nederland opgeslagen.

veiligheid In een maatschappij die sterk de nadruk legt op *veiligheid*, kan de druk groot worden om de hielprikdatabank te koppelen aan (of te gebruiken als) een forensische databank – niet alleen voor opsporingsdoeleinden, maar ook bijvoorbeeld voor identificatie bij rampen. Het doelbindingsprincipe zal in een veiligheidsmaatschappij minder belangrijk worden geacht dan veiligheid, zodat het gebruik van de hielprik voor andere doeleinden maatschappelijk aanvaardbaar kan worden geacht.[48] Wellicht belangrijker nog dan het bevolkingsbrede karakter is de verwachting dat een dergelijke maatschappij niet alleen het DNA-profiel maar ook het DNA-materiaal *zelf* zal willen opslaan, vanwege de schat aan genetische informatie die dit kan bieden. Dit DNA-materiaal zou bijvoorbeeld kunnen worden gebruikt voor risicoselectie, waarbij veroordeelden – en wellicht ook verdachten – behandeld worden aan de hand van de kennis over hun genetische eigenschappen, die bijvoorbeeld met agressie, impulsiviteit of pedofilie te maken kunnen hebben (zie variabele 6).

privacy In een *privacymaatschappij* in 2030 zal doelbinding nog steeds belangrijk zijn en zal het schot tussen hielprikdatabank en forensische databank blijven bestaan. Niettemin zal ook in dat scenario de reikwijdte van de forensische DNA-databank toenemen, vanwege het grote belang voor de opsporing;[49] de soorten misdrijven waarbij DNA-profielen mogen worden opgeslagen zullen langzamerhand worden uitgebreid. Maar in het privacyscenario worden wel perken gesteld aan hoe lang het profiel wordt bewaard, zullen alleen profielen en geen DNA-materiaal zelf van veroordeelden worden opgeslagen, en zullen beperkingen bestaan aan wie voor welke doeleinden DNA-profielen mag vergelijken.

Variabele 6: genetica en neurofarmacologie

De kennis van genen neemt langzaam maar gestaag toe. Het zijn zelden unieke genen (stukjes DNA) die verantwoordelijk voor een bepaald aspect van menselijke kenmerken, eigenschappen of gedrag, maar vrijwel steeds een complexe wisselwerking tussen meerdere genen, RNA en eiwitten; daarbij komt dan nog de invloed van omgevingsfactoren, niet alleen van opvoeding, maar ook bijvoorbeeld de positie in de baarmoeder en van voeding, die het uiteindelijke samenstel van een individu bepalen. Dit betekent dat het veelal niet mogelijk is één-op-éénrelaties te leggen tussen genen en kenmerken of gedrag. Niettemin is wel duidelijk dat genen een substantiële invloed hebben, zowel op persoonskenmreken als op bepaalde gedragskenmerken. Men kan verwachten dat in de toekomst geleidelijk meer bekend zal worden van complexen van genen die een bepaalde mate van aanleg aanduiden voor personen om bepaalde eigenschappen te ontwikkelen; zo zijn er momenteel genen bekend die 90% waarschijnlijkheid opleveren dat de drager rood haar heeft,[50] en zijn er al (vermoedelijk nog weinig betrouwbare) tests op de markt om oogkleur af te leiden uit DNA.[51] Daarbij zij opgemerkt dat er ook geluiden zijn dat niet alleen DNA, maar ook andere biometrische kenmerken zoals irissen of vingerafdrukken, onvermoede kennis zouden kunnen bieden over persoonskenmerken.[52]

[47] Zie Statewatch, 'UK: Police can keep DNA of innocent people indefinitely', September 2004, <http://database.statewatch.org/unprotected/article.asp?aid=26055>.
[48] Vraaggesprek Ulco van de Pol.
[49] Vraaggesprek Ulco van de Pol.
[50] Jobling & Gill 2004, p. 748.
[51] 'DNAPrint Announces the Release of RETINOME(TM) for the Forensic Market: Eye Color Prediction From Crime Scene DNA!', <http://biz.yahoo.com/prnews/040817/fltu014_1.html>.
[52] Hornung 2004 verwijst naar literatuur die zou suggereren dat bijvoorbeeld diabetes is af te lezen uit de iris en dat een vingerafdruk aanwijzingen kan geven over het syndroom van Down of het syndroom van Klinefelter.

Daarnaast ontstaat meer kennis over de mogelijkheden om menselijk gedrag te beïnvloeden door neurofarmacologie.[53] Zo kan een laag gehalte aan serotonine (een neurotransmitter) gepaard gaan met bijvoorbeeld agressie, depressie en slechte zelfbeheersing, en medicijnen (of drugs) zoals Prozac zijn in staat om dergelijke gevoelens en gedrag te beïnvloeden door de neurohuishouding 'op peil' te brengen. Sommigen verwachten dat de ontwikkeling in neurofarmacologie sneller – en wellicht nog grotere – gevolgen zal hebben voor de inrichting van de maatschappij dan genetica: 'Long before genetic engineering becomes a possibility, knowledge of brain chemistry and the ability to manipulate it will become an important source of behavior control that will have significant political implications.'[54]

veiligheid

Een *veiligheidsmaatschappij* zal de mogelijkheden die kennis van genetica en neurofarmacologie biedt om gedrag te kunnen inschatten en beïnvloeden ten volle willen uitnutten. Zo zal men aan de hand van genen en neurohuishouding risicoprofielen willen opmaken van personen om een inschatting te kunnen maken van bijvoorbeeld agressie, impulsiviteit of pedofilie, zodra wetenschappelijke kennis van dergelijke verbanden beschikbaar zou zijn. Ook zal op basis van die kennis nagedacht worden over verplichte behandeling van personen met een te hoog risicoprofiel, door toedienen van 'medicijnen' die de neurohuishouding meer in evenwicht brengen of, wanneer dat mogelijk zou zijn, door selectief de gewraakte genen op te sporen en uit te schakelen (zoals in huidige experimenten met 'knock-out'-muizen gebeurt). Daarbij zal doelbinding geen overwegende rol spelen: indien bij medische controles of behandelingen een 'afwijkend' of 'riskant' genen- of neuroprofiel blijkt, zal de veiligheidsmaatschappij vermoedelijk niet schromen om dergelijke informatie ook voor andere doeleinden, waaronder voorkoming van misdrijven, te gebruiken.

privacy

In een *privacymaatschappij* zal kennis over genetica en neurofarmacologie slechts met mate worden gebruikt voor andere dan medische toepassingen. Risicoprofilering zal zeer beperkt worden toegepast. Bovendien zal men terughoudend zijn met gedwongen behandeling – bijvoorbeeld door genen aan te passen, als dat technisch mogelijk zou zijn, of door proactief de neurohuishouding 'op peil' te brengen – bij personen met 'abnormale' profielen of met gebleken maatschappelijk onaanvaardbaar gedrag; immers, het belang dat de privacymaatschappij hecht aan autonomie stelt scherpe grenzen aan het ingrijpen in dat wat mensen – ook misdadigers – bij uitstek tot individueel mens maakt.

4. Veiligheid

4.1. Veiligheidscontext en -ontwikkelingen

Bescherming van *lijf, goed en eerbaarheid* speelt in 2030 onverminderd een grote rol. Indien de maatschappij zich van verzorgingsmaatschapij meer richting nachtwakerstaat ontwikkelt, zijn lijf, goed en eerbaarheid de belangrijkste hulpbronnen die individuen tot hun beschikking hebben om in hun levensonderhoud en gezondheid te voorzien – meer nog dan nu het geval is. De rol van eerbaarheid als onderdeel van veiligheid zal een steeds belangrijker rol spelen. De mobiliteit van werknemers neemt af, wellicht deels door energieschaarste, maar vooral door toenemende technische mogelijkheden om op afstand te werken en te ontspannen. Daarnaast ontwikkelt de maatschappij zich meer en meer naar een dienstenmaatschappij; veel werknemers kiezen ervoor om voor zichzelf te beginnen en hun diensten vanuit huis of dicht bij huis liggende locaties aan te bieden. De eer en reputatie van deze zelfstandigen is daarmee een belangrijke te beschermen waarde geworden. De aantasting van eer en reputatie, door bijvoorbeeld smaad en laster, zal voornamelijk plaatsvinden middels ICT. Van de overheid mag worden

[53] Zie ook Vraaggesprek Arie Rip.
[54] Fukuyama 2002, p. 42-43.

verwacht dat zij certificering voor allerlei dienstverlenende beroepen ontwikkelt of faciliteert, zodat de maatschappij zo veel mogelijk gevrijwaard blijft van charlatans. Omgekeerd zal de staat inbreuken op de goede naam van individuen stevig moeten aanpakken, naast de mogelijkheden die het civiele recht in dit opzicht biedt.

privatisering Zoals in par. 2.2 reeds is opgemerkt, zal *privatisering* van beveiliging toenemen, zij het in verschillende mate afhankelijk van de rol die de overheid op zich neemt. In de huidige maatschappij is particuliere beveiliging een grote groeimarkt,[55] en deze tendens zal doorzetten, ook in een samenleving die meer nadruk legt op privacy.[56] Een belangrijk verschil in beide scenario's zal de mate van toezicht en beperking van particuliere beveiliging zijn. Bedrijfsmatig georganiseerde particuliere opsporing valt niet onder het normeringskader van het wetboek van strafvordering. Dit brengt met zich mee dat commerciële bedrijven opsporingsmiddelen kunnen inzetten – bijvoorbeeld stelselmatige observatie – die voor de overheid niet of slechts onder strikte voorwaarden kunnen worden toegepast. Evenmin zijn zij gebonden aan ongeschreven beginselen als die van proportionaliteit en subsidiariteit.[57] De inbreuken op het privéleven van burgers die hierdoor mogelijk zijn, zullen in een veiligheidsmaatschappij makkelijker worden geaccepteerd dan in een privacymaatschappij. In het privacyscenario zal particuliere beveiliging meer in lijn worden gebracht met de normering voor overheidsbeveiliging en –opsporing, en zullen doelbinding, subsidiariteit en proportionaliteit centrale aandachtspunten zijn in het toezicht op de parctiuliere beveiligingsbureaus.

strafrecht Een andere veiligheidsgerelateerde ontwikkeling is dat de huidige maatschappij zich kenmerkt door een toenemende *werkingssfeer van het strafrecht*, een 'criminalisering van de maatschappij'.[58] Dit uit zich enerzijds in een uitbreiding van strafbaarstellingen, vooral ook in de voorfase van strafwaardig handelen. Zo neemt de strafbaarstelling van voorbereidingshandelingen die op zichzelf geen schade aanrichten, toe, bijvoorbeeld bij computerdelicten en verkeersdelicten, evenals bij samenspanning tot (terroristische) misdrijven.[59] Anderzijds uit zich deze tendens in de uitbreidingen van opsporingsbevoegdheden die steeds meer ook ten opzichte van onverdachte burgers kunnen worden uitgeoefend; voorbeelden zijn aftappen, observatie en het opvragen van allerhande gegevens over burgers.[60]
Het ligt in de rede dat deze tendens zich zal voortzetten. Juist doordat de techniek het mogelijk maakt allerlei handelingen in de voorfase van strafwaardig handelen te detecteren, zal de roep om die detectie uit te voeren toenemen en vermoedelijk ook gepaard gaan met de wens om gedragingen in dat voorveld strafbaar te stellen. Het valt te verwachten dat de huidige ontwikkeling van agressiedetecterende camera's zal leiden tot een definitie van wat als agressiviteit in de openbare ruimte wordt beschouwd (denk aan: armzwaaien, hollen, open mond, vuistballen, middelvingers opsteken) ten behoeve van handhaving van de openbare orde bij bijvoorbeeld demonstraties. Dit zal gepaard kunnen gaan met ordemaatregelen als preventief hechten bij vertonen van agressief gedrag in het openbaar. Denkbaar is echter ook dat de detectiemogelijkheid leidt tot strafbaarstelling van dergelijk gedrag, en dat de enkele vaststelling daarvan met een agressiedetecterende camera een bestuurlijke boete zal opleveren. Wanneer de camera daarbij nog gekoppeld zou worden aan automatische gezichtsherkenning, kan een systeem worden ingevoerd van automatische afdoening, vergelijkbaar met de huidige sanctionering van te hard rijden. Voor een privacymaatschappij is een dergelijke ontwikkeling ondenkbaar, omdat camerabewaking daarin niet individualiseerbaar zal plaatsvinden, maar voor een veiligheidsmaatschappij is dit scenario niet denkbeeldig.

[55] Zie bijvoorbeeld Hoogenboom 2000.
[56] Vgl. het SCR 2004, p. 480-482: 81,6% van de bevolking verwacht dat in 2020 burgers meer zelf verantwoordelijk zijn voor de veiligheid in hun woonomgeving. En 88,7% verwacht dat toezicht meer door particuliere beveiliging wordt toegepast; een meerderheid vindt dat ook wenselijk.
[57] Zie hierover, met name voor wat betreft kritiek op huidige gebreken in controle en toezicht, Groenhuijsen/Knigge (red.), Strafvordering 2001, derde deelrapport p. 60-63 en p. 689-749.
[58] Koops 2003.
[59] Koops & Prins 2003.
[60] Zie bijvoorbeeld Stevens, Koops & Wiemans 2004.

slachtoffers In het debat over veiligheid is de afgelopen decennia in toenemende mate ook zelfstandige aandacht besteed aan de *positie van slachtoffers* van misdrijven. Dit heeft interessante nieuwe inzichten opgeleverd, die zijn ondersteund door de resultaten van empirisch onderzoek. Zo blijken de onveiligheidsgevoelens van mensen die zelf slachtoffer zijn geweest aanmerkelijk groter te zijn dan bij anderen het geval is. Nog opmerkelijker is het verschijnsel dat wordt aangeduid als 'herhaald slachtofferschap': een relatief klein deel van alle slachtoffers blijkt te worden getroffen door een onevenredig groot deel van de misdrijven. Dit verschijnsel doet zich voor bij alle typen delicten, dus zowel bij vermogens- als bij geweldsmisdrijven. Beleidsmatig heeft dit geleid tot het zoeken naar nieuwe beveiligingsmethoden met technische hulpmiddelen. Als interessant voorbeeld kan worden gewezen op rechtstreekse verbindingen tussen de woning van het slachtoffer van een delict als 'stalking' en het politiebureau door middel van een alarmknop.[61] Voor de toekomstscenario's betekent deze ontwikkeling dat in 2030 meer aandacht zal zijn, zowel wetenschappelijk als beleidsmatig, voor de bescherming van (potentiële) slachtoffers, waarbij meer nadruk wordt gelegd op risicofactoren voor slachtofferschap. Te denken valt aan sociale en economische, maar wellicht ook aan genetische, factoren die een rol kunnen spelen bij (herhaald) slachtofferschap. Groepsprofilering en daarop gebaseerde preventiemaatregelen gericht op "verhoogde slachtofferrisicogroepen" zullen worden ingezet. Gepoogd zal worden beveiligingsmaatregelen meer gedifferentieerd in te zetten; aangezien (gebrek aan) beveiliging echter zelf een mogelijke risicofactor is voor (herhaald) slachtofferschap, zal de personalisatie van beveiliging voortdurend geactualiseerd en aangepast moeten worden.

Voor wat betreft *misdaad* verwachten wij geen opzienbarende ontwikkelingen; vanzelfsprekend zal de aard en intensiteit van zowel kleine als zware criminaliteit doorlopend veranderen, maar dit betreft geleidelijke ontwikkelingen die geen fundamenteel ander beeld zullen opleveren voor de maatschappij van 2030. Niettemin verwacht de bevolking in 2004 wel dat problemen rond veiligheid en criminaliteit in 2020 groter zullen worden, waarbij vooral geweldscriminaliteit en computercriminaliteit hoog scoren in de toenameverwachting.[62]

terrorisme Op het gebied van *terrorisme* zijn belangrijke ontwikkelingen te verwachten. Het risico op een terroristische aanval neemt toe, door twee ontwikkelingen. In de eerste plaats is het nu reeds mogelijk met minimale middelen maximale schade aan te richten; de aanslagen op de Tweelingtorens in New York op 11 september 2001 kostten een fractie van de materiële schade, om maar te zwijgen van de immateriële schade, en voor de aanslagen in Madrid van 11 maart 2004 bleek slechts $10.000 nodig.[63] Deze mogelijkheid zal in de toekomst niet minder worden; en daar komt dan nog de dreiging bij van een biologische of nucleaire aanslag, die weliswaar meer kost en moeilijker uitvoerbaar is dan genoemde aanslagen, maar waarbij het aantal slachtoffers ook enorm veel groter kan zijn.[64]
In de tweede plaats is er sprake van een andersoortig terrorisme dan we kenden uit de jaren 1970-2000, dat veelal een duidelijk en concreet politiek doel had. Nu is het 'megalomaan hyperterrorisme' in opkomst, dat veel ongerichter is en geen concreet doel heeft, maar meer apocalyptisch van aard is.[65] Bovendien is dit terrorisme afkomstig van moeilijk definieerbare – en dus traceerbare – actoren. Tezamen levert dit een nieuw paradigma op van 'terrorist groups capable of wreaking havoc of the kind that only states could previously inflict, but without the accountability of states'.[66]

[61] Zie <www.victimology.nl/onlpub/otherdocs/rv-bibliography.doc> en M.S. Groenhuijsen in *D&D* 2004, p. 111-117 voor cijfers en verwijzingen.
[62] SCR 2004, p. 479-480.
[63] <http://news.bbc.co.uk/2/hi/americas/3606384.stm>.
[64] Vgl. Vraaggesprek Buruma.
[65] De term 'megalomaan hyperterrorisme' is van Ehud Spinzrak, aangehaald in Dershowitz 2002, p. 10.
[66] Dershowitz 2002, p. 11.

In de huidige context heeft dat geleid – en leidt dit nog steeds – tot een stroom maatregelen van terrorismebestrijding.
Deze maatregelen zullen niet, zoals soms wordt voorgespiegeld door voorstanders, tijdelijk van aard zijn, maar ze worden waarschijnlijk deel van de permanente textuur van ons juridische en politieke systeem.[67] Het terugdraaien van of stoppen met wettelijke veiligheidsmaatregelen lijkt in de praktijk weinig realistisch. Een belangrijke ontwikkeling is ook dat het de maatregelen weliswaar worden ingevoerd als 'terrorismerecht', maar vaak ook direct toepasbaar worden in het reguliere strafrecht, op niet-terrorisme-gerelateerde feiten. Deze verwevenheid van terrorismebestrijding met misdaadbestrijding zal alleen maar toenemen.
Een wezenlijk onderdeel van het scenario van 2030 is dan ook hoe de maatschappij zal reageren op een grootschalige terroristische aanslag in of nabij Nederland. Deze reactie zal illustratief zijn voor de omgang van de maatschappij met veiligheid en privacy, zodat we binnen dit onderzoek ervan uitgaan dat tussen nu en 2030 een dergelijke aanslag in Nederland zal plaatsvinden. Een belangrijke keuze in dat licht is of de maatschappij pro-actief daarop anticipeert door veiligheidsmaatregelen, die deels ten koste zullen gaan van privacy, of dat gewacht wordt tot maatregelen re-actief op de aanslag. In het laatste geval is er een groter risico dat onder populistische druk de maatschappij met minder reflectie en bedachtzaamheid maatregelen zal invoeren ten koste van privacy. Er is dus een enigszins paradoxale situatie dat een maatschappij die grote nadruk op privacy legt, op lange termijn een zeker risico loopt om – na een zware terroristische aanslag – een groter deel van de privacy in te leveren ten behoeve van veiligheid(sgevoel) dan een maatschappij die op voorhand al de nadruk legt op veiligheid.

vertrouwen

Een ander aspect van de verwachte terreuraanslag, gekoppeld aan de nog steeds individualiserende en multiculturaliserende maatschappij, is dat het daarmee gepaard gaande verlangen naar veiligheid en de angst voor onbekenden knagen aan het *vertrouwen* van burgers in de overheid, van burgers onderling en van burgers tegenover private organisaties. Er ontstaat een breed gedragen behoefte aan identificeerbaarheid van mensen en instellingen, niet alleen tegenover het bevoegd gezag maar ook in het dagelijkse maatschappelijke verkeer. Ook zal er behoefte ontstaan aan nieuwe manieren om de geloofwaardigheid en betrouwbaarheid te controleren van individuen, beroepsbeoefenaren en organisaties. Er zullen tal van private en/of overheidsinitiatieven worden genomen om op grote schaal identificaties en betrouwbaarheidscontroles te laten uitvoeren die het vertrouwen in alledaagse handelingen, van winkel tot school en horeca, wederzijds beogen te verhogen.
Daarbij staat in toenemende mate de doelbinding van justitiële registers onder druk. De justitiële antecedenten van burgers zijn thans in beginsel nog vertrouwelijk:[68] alle politie- en justitiecontacten worden vastgelegd in verschillende dossiers, maar de raadpleging daarvan is alleen onder strikte voorwaarden mogelijk, en grotendeels beperkt tot overheidsinstanties. Er zal toenemende druk worden uitgeoefend, van verschillende kanten, om dit regiem te versoepelen. Burgers zouden zich veiliger voelen als bijvoorbeeld in de omgeving van scholen algemeen bekend zou zijn welke individuen zich ooit schuldig hebben gemaakt aan zedendelicten, of wanneer zij kunnen nagaan dat de leraren, sporttrainers, taxi-chauffeurs en privébeveiligers met wie zij of hun kinderen in aanraking komen, nooit veroordeeld zijn geweest voor een strafbaar feit.

In het verlengde hiervan zal er ook meer aandacht zijn voor de rol van het onderwijs. Als er ergens in de maatschappij gelegenheid is om structureel iets te doen ter voorkoming van misdaad, dan is dat het onderwijs. Volgens het SCR 2004 verwacht 81,6% van de bevolking dat in 2020 meer aandacht zal zijn binnen het onderwijs voor het voorkómen van criminaliteit, en maar liefst 98,2% vindt dat ook wenselijk.[69]

[67] Dershowitz 2002, p. 11.
[68] Zie de Wet justitiële gegevens en het daarop gebaseerde Besluit justitiële gegevens.
[69] SCR 2004, p. 481. Voor wat betreft de rol van opvoeding verwacht 67,1% dat daarbij meer aandacht zal zijn voor

Voor de maatschappij van 2030 zal dan ook veel afhangen van de wijze waarop het basis- en voortgezet onderwijs wordt ingericht, met name ook van de veiligheidsmaatregelen die scholen zelf nemen en de uitstraling die daarvan uitgaat. Voor het veiligheidsscenario (met een nachtwakerstaat) en een privacyscenario (met een optredende overheid) zal daarbij ook een uiteenlopende invulling van het onderwijs – meer of minder privaat onderwijs; meer of minder verplichte inrichting van het curriculum – een rol spelen.

4.2. Veiligheidsvariabelen

Variabele 7: controle van daders

Een huidige tendens is een toenemende greep van het strafrecht op de maatschappij, zowel qua strafbaarstellingen als qua reikwijdte van opsporingsbevoegdheden. Daarbij neemt ook de roep toe om misdadigers na het uitzitten van de straf te blijven volgen of anderszins te proberen af te houden van recidive. Voorbeelden daarvan zijn de uitbreiding van de DNA-databank (zie par. 3.2), die nadrukkelijk bedoeld is om veroordeelden af te schrikken om opnieuw in de fout te gaan, de uitvergrote media-aandacht voor TBS'ers die op proefverlof misdrijven plegen, voorstellen om foto's van pedofielen of winkeldieven op Internet te plaatsen, en de ideeën die her en der gelanceerd worden om veroordeelden die na de straf vrijkomen uit te rusten met elektronisch toezicht. De techniek is daarvoor beschikbaar: met een chip (geïmplanteerd of op een niet-verwijderbare enkelband), GPS-ontvangertje en zendertje kan men continu volgen of een veroordeelde pedofiel in de buurt rondhangt van een school, bijvoorbeeld.[70]

veiligheid De tendens om (potentiële) misdadigers te volgen en aldus te weerhouden van het plegen van (nieuwe) misdrijven zal zich doorzetten – niet in het minst omdat de techniek daartoe toenemende handvatten biedt. Wel zal de mate waarin deze tendens zich ontwikkelt verschillen naar gelang de roep om veiligheid of privacy. Een *veiligheidsmaatschappij* anno 2030 zal vermoedelijk sterke nadruk leggen op controlemogelijkheden die gericht zijn op preventie. Dit geldt zowel voor veroordeelden die weer 'losgelaten' worden op de maatschappij als voor personen die nog nooit veroordeeld zijn voor een strafbaar feit, maar waarvan het profiel een verhoogd misdaadrisico laat zien, gebaseerd op genetische, sociale en gedragskenmerken. Zij zullen gechipt en wel onder permanent elektronisch toezicht staan: hun locatie wordt onverwijld doorgegeven aan een volgsysteem, wellicht gekoppeld aan een niet-verwijderbare webcam die ergens aan het lichaam is bevestigd. Denkbaar is ook dat de geïmplanteerde chip lichaamsfuncties meet, zoals hartslag en bloeddruk, maar ook veranderingen in hormoonspiegel en neurotransmitters, waardoor indicaties worden doorgegeven van een mogelijke toestand van grote opwinding, depressie of lust. Technisch zal het ook mogelijk zijn om signalen terug te sturen naar de gechipte persoon, die bijvoorbeeld een pijnsignaal naar de hersenen sturen of wat extra neurotransmitters loslaten waardoor de persoon acuut kalmeert. Het laatste kan natuurlijk ook off-line worden ingebouwd, door een geïmplanteerd zelfregulerend hormoonhuishoudingsfabriekje die emotionele pieken en dalen aftopt (vgl. par. 3.2 onder Genetica en neurofarmacologie). Een andere verschijningsvorm van deze tendens in de veiligheidsmaatschappij is noemen & verdoemen: veroordeelden waarbij de recidivekans hoog wordt ingeschat zullen publiekelijk bekend worden gemaakt, met foto's op Internet, gemeentehuizen, scholen, winkels.

privacy In een *privacymaatschappij* anno 2030 zal men terughoudend zijn met dergelijke maatregelen, hoewel wij verwachten dat ook in een dergelijke maatschappij

het voorkómen van criminaliteit; 98,9% vindt dat ook wenselijk.

[70] Vgl. de proef die in oktober 2004 werd voorgesteld om gevangenen uit een jeugdinrichting in Zutphen uit te rusten met een arm- of enkelband, waardoor op afstand te volgen is waar zij zich bevinden. 'Het nieuwe volgsysteem geeft ruime bewegingsvrijheid, maar een meldkamer houdt via een satelliet bij waar de gevolgde persoon zich bevindt.' Aldus *Privacy & Informatie* 2004/6, p. 271, gebaseerd op *de Volkskrant* 7 oktober 2004.

aandacht zal zijn voor maatregelen die potentiële recidivisten beogen te weerhouden van nieuwe misdaden. Dit zal dan eerder de vorm aannemen van een vroegalarmsysteem dat, op basis van profielen met een wetenschappelijk bewezen hoog risico op het plegen van ernstige misdrijven (wellicht bij bepaalde genetische afwijkingen of een van nature zeer depressieve hormoonspiegel) mensen aanwijst die in aanmerking komen voor een vrijwillig begeleidingstraject, waarin bijvoorbeeld de negatieve hormoonhuishouding wordt bijgesteld. Het ex-post volgen van vrijgelaten veroordeelden zal in een privacymaatschappij niet of slechts zeer spaarzaam worden toegestaan, vanuit de gedachte dat de straf is uitgezeten en men zich dan vrijelijk moet kunnen bewegen in de maatschappij. Bovendien maken maatregelen die een veiligheidsmaatschappij accepteert, zoals het chippen van vrijgelaten veroordeelden en het permanent volgen van hen, voor een privacymaatschappij een te grote inbreuk op lichamelijke, ruimtelijke en informationele privacy om deze te kunnen invoeren.

Variabele 8: meewerken door burgers aan opsporing
Een vitaal kenmerk van het huidige veiligheidsbeleid is dat burgers wel bevoegd, maar in menig opzicht niet verplicht zijn om mee te werken aan het opsporen van strafbare feiten. Voor de afweging van veiligheids- en privacy-aspecten is het van groot belang of dit in de toekomst zo zal blijven. Nederland kent momenteel bijvoorbeeld geen algehele aangifteplicht (zie art. 160 e.v. WvSv).

veiligheid In het *veiligheidsscenario* zal overwogen worden om een algemene aangifteplicht te introduceren, teneinde zoveel mogelijk misdrijven zo snel mogelijk op te kunnen sporen. Dit levert een grote toevloed van zaken op, waaronder ook 'bagatelzaken', die het justitiële apparaat sterk belast. Grote financiële investeringen zijn nodig om alle aangiftes te beoordelen en af te handelen, althans wanneer de maatschappij hetzelfde niveau van strafrechtelijke handhaving ten opzichte van de huidige opgespoorde en vervolgde delicten wil bereiken. In de praktijk wordt met veel aangiftes dan ook weinig gedaan, maar in de publieke beeldvorming zal de aangifteplicht als een belangrijke bijdrage aan veiligheid worden gepresenteerd.

privacy In het *privacyscenario* wordt een algemene aangifteplicht afgewezen. Uitbreiding van aangifteverplichtingen van gewone burgers heeft immers een grote weerslag op de privacy van mensen. Delicten die thans informeel worden opgelost – of om andere redenen niet aan de politie worden gemeld, zoals bedreigingen – zouden dan bij justitie bekend worden en worden geregistreerd. De privacymaatschappij van 2030 wijst dit af. Daarentegen zal in het privacyscenario de tendens van anonieme misdaadmeldpunten – Meld Misdaad Anoniem[71] – zich doorzetten, aangezien in deze maatschappij, die duidelijke beperkingen stelt aan de mogelijkheden voor politie en justitie om proactief of reactief misdrijven op te sporen, behoefte bestaat aan aanvullende informatiebronnen die vrijwillig, en met behoud van privacy, de opsporing van dienst zijn.

5. Privacy

5.1. Privacycontext en -ontwikkelingen

In 2030 zal men alle tegenwoordig onderscheiden dimensies van privacy nog steeds belangrijk vinden. Ruimtelijke, fysieke en relationele privacy blijven onverkort gewaardeerd. Over informationele privacy zal men echter anders gaan denken dan in 2005. Door de alomtegenwoordigheid van kleine computers, sensoren en netwerken en de volledige integratie van deze apparaten en netwerken in het dagelijkse en professionele leven, zijn mensen eraan gewend geraakt dat er voortdurend enorme hoeveelheden data over hun gedrag (ook het meest intieme) worden gegenereerd, opgeslagen en verwerkt. Tegelijkertijd neemt het hergebruik

[71] Zie <http://www.meldmisdaad.nl>, dat automatisch doorkoppelt naar <http://www.meldmisdaadanoniem.nl/>.

van geanonomiseerde gegevens hand-over-hand toe. Door deze twee tendensen zal informationele privacy steeds minder worden geïnterpreteerd in termen van de bescherming van persoonsgegevens als brongegeven in strikte zin. In plaats daarvan zal informationele privacy meer en meer worden uitgelegd als een notie die betrekking heeft op de bescherming van personen tegen allerlei uiteenlopende consequenties van bepaalde toepassingen van informatie die aan die personen gerelateerd kan worden. Aldus zal wat van oudsher als informationele privacy wordt aangeduid, minder ervaren worden als onderdeel van privacy, maar meer als een zelfstandig te waarderen belang van gegevensbescherming, waarbij nadruk ligt op transparantie en autonomie.[72] (Zie nader par. 5.2.)

lichaam

Lichamelijke privacy blijft relevant in 2030.[73] De burger zal het nog steeds belangrijk vinden zelf te kunnen bepalen wat hij met zijn lichaam doet: hij hoeft geen invloeden te dulden van buitenaf die zijn lichaam dwingen iets anders te doen of te zijn dan hij zelf beoogt. Wel zal de invulling van het begrip van lichamelijke integriteit gaan veranderen: het functioneren van het lichaam wijzigt geleidelijk aan door intelligente kleding, chip-implantaten, brein-machine-combinaties en veranderingen in het lichaam door bijvoorbeeld nanotechnologie. Deze ontwikkelingen betekenen een toenemende integratie van techniek en het lichaam. Zonder direct aan bionische mensen of robocops te denken, kunnen we wel het toekomstbeeld verwachten van mensen waarvan technologie op en in het lichaam in steeds grotere mate de 'natuurlijke' lichamelijke functies bevordert, verbetert, herstelt of uitbreidt, in eerste instantie voor medische doeleinden, maar in tweede instantie ook omdat het leuk of anderszins nuttig is.[74] Waar tot nu toe het menselijk lichaam als uniek en absoluut verschijnsel wordt gezien en ervaren, zal in de toekomst een minder harde scheidslijn zijn aan te brengen tussen mens en machine. Voor het grondrecht op lichamelijke integriteit valt te verwachten dat iemand de ingebouwde technologie als onlosmakelijk onderdeel van zijn lichaam zal beschouwen. Zoals chip-implantofiel en cyborgonderzoeker Kevin Warwick zijn eigen ervaring met een chip-implantaat beschrijft: 'The biggest surprise for me during the experiment was that I very quickly regarded the implant as being "part of my body", a feeling shared with most people who have a cochlea implant or a heart pacemaker.'[75]
Voor een veiligheidsmaatschappij opent het verschijnsel van mens-machine-combinaties mogelijkheden – op lange termijn – om mensen op afstand fysiek te beïnvloeden, maar ook om het lichaam van mensen op afstand 'uit te lezen', bijvoorbeeld de informatie die is opgeslagen op geïmplanteerde medische chips die periodiek de bloeddruk, hartslag en andere lichamelijke functies meten en opslaan.

cyborgs

Ook is relevant hoe we ons begrip van het grondrecht op lichamelijke integriteit zullen toepassen op mens-machine-combinaties of cyborgs waarbij in toenemende mate de machine meer invloed heeft op het functioneren van de persoon als geheel. 'The main point arising from this is: when an individual's consciousness is based on a nervous system that is part human part machine, questions can be raised as to the human/cyborg character of their moral choices, their identity, and conception of ethics. As a consequence cyborgs may well regard humans with an air of superiority.'[76] Wat betekent het verschijnsel cyborg voor ons begrip van de menselijke autonomie, dat nauw verweven is met het recht op privacy? Zoals

[72] Zie Vraaggesprek Van de Pol.
[73] Zie uitgebreid hierover Koops, Van Schooten & Prinsen 2004.
[74] 'Overall therefore, from a human point of view, a number of distinct advantages can be accrued by becoming a cyborg, as long as human brain advantages such as resilience, tolerance to ambiguity, etc. are preserved. In particular when a human brain is linked, via an implant, to a computer, it opens up the power of the machine to the implanted individual. A human receiving an implant may well then be able to: use their computer part for rapid maths; call on a high speed, internet knowledge base; have memories they have not had; sense the world in a plethora of ways; conceive reality multi-dimensionally; communicate by thought alone. All of the above might appear to be valid reasons for an individual human to enhance his abilities through cyborg technologies.' Warwick 2002.
[75] Warwick 2002.
[76] Warwick 2002.

Warwick aangeeft: 'From my own latest implant research, when connected directly with technology I am aware that there is a loss of human autonomy';[77] wanneer we dit doortrekken naar een maatschappij waarin het menselijk lichaam nauw verweven is met technische implantaten, betekent dit mogelijk een fundamentele herbezinning op het idee van de menselijke autonomie en privacy.
Voor de scenario's van 2030 houden wij deze langetermijnvragen op de achtergrond, aangezien het vermoedelijk in 2030 nog niet zover zal zijn dat cyborgs volledig operationeel zijn. Het verdient echter wel aanbeveling de ontwikkelingen op het gebied van mens-machine-combinaties nauwgezet te volgen en tijdig maatschappelijke en politieke discussies te voeren over fundamentele vragen als de reikwijdte van lichamelijke integriteit over ingebouwde of verbonden techniek en de rechtssubjectiviteit van mens-machine-combinaties.[78]

communicatie Voor de *relationele privacy* zijn diverse scenario's mogelijk. De invloed van nieuwe communicatiemiddelen zoals mobiele telefonie, e-mail en Internet verandert de perceptie van mensen aangaande de vertrouwelijkheid van hun communicatie. Enerzijds lijkt de beschermingsbehoefte van vertrouwelijke communicatie in de dagelijkse praktijk momenteel steeds meer te worden gerelativeerd; zie bijvoorbeeld het door vele personen zonder schroom in het openbaar communiceren van privé-zaken via mobiele telefoon. Deze tendens kan verder doorzetten, waardoor mensen in de toekomst geneigd zullen zijn nog in geringe mate waarde te hechten aan het recht op vertrouwelijke communicatie. De beschermwaardigheid van het grondrecht op vertrouwelijke communicatie kalft daarmee in dit scenario geleidelijk af. Anderzijds stellen we ook vast dat de scheidslijn tussen enerzijds de relationele privacy (in de zin van het in vrijheid aangaan en onderhouden van relaties) en anderzijds de vertrouwelijke communicatie, met de oprukkende populariteit van elektronische communicatiediensten steeds verder vervaagt. Mensen gaan ook hun intieme relaties steeds vaker via elektronische media aan,[79] om deze daarna ook via deze media te onderhouden. Een en ander zou kunnen betekenen dat de waarde die mensen gaan hechten aan vertrouwelijke communicatie, ook binnen groepsverband – denk aan jongeren, sterk samenhangt met het recht om in vrijheid en zonder inmenging van buiten relaties aan te gaan en te onderhouden. Wanneer het recht om in vrijheid relaties aan te gaan blijvend als belangrijk wordt gepercipieerd, waarbij het recht op vertrouwelijke communicatie als essentieel onderdeel daarvan wordt beschouwd, zal ook de beschermwaardigheid van dit laatste grondrecht van groot belang blijven.

5.2. Privacyvariabelen

Variabele 9: informationele privacy

veiligheid In het veiligheidsscenario zullen de Wet bescherming persoonsgegevens en de onderliggende uitgangspunten daarvan niet langer als leidend regime voor de omgang met persoonsgegevens worden erkend. Het uitgangspunt voor omgang met gegevens is dat in beginsel alles gebruikt mag worden, tenzij er overwegende belangen zijn om dat niet te doen. Het belang van het criterium doelbinding wordt losgelaten omdat het niet langer als realistisch wordt gezien dat bepaalde vormen van gegevensverwerking als het ware op voorhand reeds buiten het verwerkingsbereik worden geplaatst (omdat deze niet in overeenstemming zouden zijn met het doel waarvoor de gegevens in eerste instantie werden verkregen). In het veiligheidsscenario is het mogelijk, door doelbinding als uitgangspunt los te laten, flexibel op de concrete maatschappelijke realiteit in te springen. De

[77] Warwick 2002.
[78] 'Thus, we might see some interesting battles erupting over how or whether to classify intelligent machines as a species, especially if we tried to control their intellectual property, turn them off, sue them, or give them rights and bank accounts.' Mulhall 2002, p. 108-109.
[79] Zie de populariteit van *dating sites* en digitale groepsverbanden van jongeren. Vgl. 'toothing': het in bijvoorbeeld treincoupés uitzenden via Bluetooth van een (geanonimiseerde) uitnodiging tot seks, die door mobieltjes in de nabije omgeving opgevangen kan worden. Zie Laurens Verhagen, 'Nieuwe Bluetooth-rage leidt tot snelle seks', *Webwereld* 20 april 2004, <http://www.webwereld.nl/nieuws/18326.phtml>.

beschermwaardigheid van persoonsgegevens kan als het ware automatisch worden gerelativeerd indien er op een bepaald moment gerechtvaardigde belangen binnen de samenleving zijn die vergen dat het privacybelang van burgers opzij wordt gezet.

privacy

In het privacyscenario blijft men vasthouden aan de nu gangbare beginselen voor *fair information practices* (zoals doelbinding en transparantie) als waarborg tegen bepaalde ongerechtvaardigde vormen van gegevensverwerking. Informationele privacy wordt daarbij gezien als een regime waarin de kern van het recht niet zozeer ligt in het te beschermen object (persoonsgegevens), maar waarbij het primair gaat om het beschermen van mensen tegen onnodige, buitenproportionele of ongerechtvaardigde betrekkingen. Kortom, in dit scenario wordt telkens beoordeeld of een verwerking, gegeven de belangen die in het concrete geval aan de orde zijn, gerechtvaardigd is. Dit betekent dat bepaalde vanuit veiligheidsoverwegingen gewenste vormen van gegevensverwerking (zoals de uitwisseling van gegevens tussen bepaalde instanties) in strijd zullen zijn met het wettelijk regime en niet toelaatbaar zijn; slechts voor ernstige gevallen of situaties zal wetgeving worden aangepast om het regime van gegevensbescherming te doorbreken. Flexibel inspringen op een bepaald veiligheidsbelang zal daarmee niet altijd te realiseren zijn. Daar staat tegenover dat burgers over het algemeen zorgvuldiger behandeld worden in het maatschappelijk verkeer, omdat niet te onpas hun gegevens in verband worden gebracht met veiligheidsrisico's waardoor zij – bijvoorbeeld op basis van groepsprofielen – onterecht een bepaald stempel opgedrukt krijgen.

Variabele 10: ruimtelijke privacy

woning

De ruimtelijke privacy legt momenteel een grote nadruk op het huisrecht: de bescherming van de woning. Weliswaar is er ook een zekere aanspraak op privacy op de werkplek en in de openbare ruimte, maar de nadruk ligt op de woning als plaats waar iemand onbevangen zichzelf moet kunnen zijn. Maar in 2030 is de woning substantieel anders van karakter dan nu. Het huis van de toekomst is een huis dat steeds elektronischer wordt en meer en meer wordt ingebed in een intern en extern computernetwerk. Het huis wordt meer dan ooit een opslagplaats voor het persoonlijke verleden van de bewoner. Het digitale geheugen is altijd en overal in het huis oproepbaar, en zal dat ook van buitenaf zijn, via het Internet. Het digitale geheugen zal ook extern kunnen worden opgeslagen – voor de bewoner maakt het immers niet uit waar het opslagmedium zich bevindt. Mede daardoor vervaagt de scheiding tussen huis en buitenwereld. Niet langer zijn de fysieke muren een daadwerkelijke afscherming van binnenshuis en buitenshuis. De woning wordt onderdeel van een netwerk, waarbij processen in de woning van buitenaf raadpleegbaar en stuurbaar zijn, en waarbij de buitenwereld meer dan ooit de huiskamer binnenkomt. Daarmee zal ook de functie van de woning geleidelijk aan veranderen: werk en gemeenschapsactiviteiten zullen vaker vanuit de woning worden uitgevoerd. Vermoedelijk zal dit ook gepaard gaan met een omgekeerde ontwikkeling: waar de buitenwereld de woning binnendringt, zal ook de woning de buitenwereld gaan verkennen. Iemand zal meer en meer elementen van de woning meenemen wanneer hij rondreist in het openbaar.[80]

Het huis van de toekomst zal daarmee ook eenvoudiger van buitenaf waar te nemen zijn: de muren en gordijnen schermen de woning niet langer af tegen pottenkijkers. De straling van allerlei apparaten (vooral van draadloze verbindingen) kan van buitenaf eenvoudig worden opgevangen. Ook kan via het computernetwerk meer informatie worden vergaard over wat zich in de woning bevindt en afspeelt, via het binnendringen in de computer of door het aftappen van telecommunicatie (bijvoorbeeld van koelkastbestellingen of het digitale archief van vakantiefoto's). Zowel politie en ivd's als hackers kunnen hiervan profiteren. Hoewel techniek ook de kennisname van buitenaf kan tegengaan, zal het huis in de toekomst waarschijnlijk in toenemende mate transparant worden.

[80] Zie uitgebreid hierover Koops, Van Schooten & Prinsen 2004.

veiligheid

Dit roept de vraag op of in 2030 de ruimtelijk privacy nog primair in de woning kan of moet worden gezocht. Voor een veiligheidsmaatschappij zal het transparant worden van de woning niet als overwegend probleem worden ervaren: een afgeschermde plaats waarin onzichtbaar dingen kunnen gebeuren wordt in een dergelijke maatschappij relatief minder op prijs gesteld dan het veiligheidsgevoel dat een overal aanwezig toezicht oproept. Dit geldt a fortiori voor semi-publieke ruimtes als werkplaatsen, winkels en privéterreinen, waar het (camera)toezicht alomtegenwoordig zal kunnen zijn. Feitelijk is er in een dergelijke maatschappij weinig ruimte om zich daadwerkelijk volledig terug te trekken: er zal altijd enige vorm van controle zijn, al is het maar door de mogelijkheid dat achteraf gegevens (beelden, geluiden) worden opgeroepen van wat iemand ergens heeft gedaan. Geheel verdwijnen kan de ruimtelijke privacy echter niet: ook in een veiligheidsmaatschappij zal men behoefte hebben om bepaalde activiteiten in de privésfeer te verrichten, met name religieuze en seksuele handelingen. Het monitoren van woningen zal daarom niet direct de vorm aannemen van permanent cameratoezicht in alle woningen. Wel zal de mogelijkheid bestaan om, waar mensen vrijwillig camerainstallaties aanbrengen – denk aan ouderen in aanleunwoningen en jongeren met webcams op kamers – een verplichte opslag in te bouwen van enkele weken in deze camera's, zodat achteraf beelden ter beschikking kunnen staan voor justitie of ivd's. Het scenario van *1984* met een permanent cameratoezicht in de woning is niet realistisch, maar een tussenvorm van beperkt visueel of auditief toezicht in de woning lijkt ons niet ondenkbaar in een maatschappij die sterke nadruk legt op veiligheid.

privacy

In een privacymaatschappij zal de woning nog in belangrijke mate een plaats vormen om onbevangen jezelf te zijn. Dat wil zeggen dat de woning weliswaar naad- en draadloos ingebed is in een netwerk, maar dat er duidelijke waarborgen, zoals doelbinding en transparantie, bestaan voor wie in welke gevallen toegang krijgt tot gegevens van bijvoorbeeld de koelkast, wasmachine of centrale thuiscomputer. Daarbij zal ook sterke aandacht bestaan voor de elektronische beveiliging van het huisnetwerk: privacy en veiligheid binnen de woning gaan in dit scenario hand in hand. Meer dan in het veiligheidsscenario zullen bewoners hulpmiddelen hebben om zich te beveiligen tegen hackers of opdringerige marketingbedrijven; in het veiligheidsscenario is er minder plaats voor die technieken omdat zij tegelijk met hackers ook beveiliging bieden tegen de overheid.[81]

6. Op naar de toekomst

Met de beschreven contexten, ontwikkelingen en variabelen in het achterhoofd, is het mogelijk scenario's te schetsen van mogelijke toekomsten. In het tweede deel van dit rapport geven we twee verhalen op basis van de bevindingen uit deel I. Deze toekomstscenario's zijn illustratief en dienend bedoeld, dat wil zeggen dat zij op luchtige wijze een verhalend beeld schetsen van mogelijke toekomsten aan de hand van onze bevindingen en verwachtingen rond maatschappij, techniek, veiligheid en privacy. Het is daarbij allerminst de bedoeling uitputtend te zijn en alle ontwikkelingen en variabelen aan bod te laten komen: de verhalen beogen veeleer een sfeerbeeld te geven dat lezers prikkelt om na te denken over de toekomst.

[81] Een prototype van dit fenomeen is de discussie rond cryptografie, een techniek om gegevens af te schermen tegen kennisneming door derden. Overheden hebben in de jaren negentig vele voorstellen gedaan voor het aan banden leggen van deze techniek, uit vrees voor belemmering van opsporingsdiensten. Zie Koops 1998.

Deel II. Twee toekomstscenario's

A. Een veiligheidsscenario

Dramatis Personae

- Elles de Vries (40), medewerker bij een beveiligingsbedrijf
- Hans Hollander (45), chirurg, samenwonend met Elles
- Xa4 de Vries (14), zoon van Elles en Hans

Den Haag, Haviklaan 6, donderdag 2 maart 2030, 07.45 uur
Het had niet veel gescheeld of Hans was alweer niet aan het ontbijt verschenen. Hij kijkt naar zijn vrouw Elles en zoon Xa4 die al een kwartier op hem zitten te wachten aan de tafel in de keuken van hun wooneenheid in Den Haag. Bij de familie Hollander is het de gewoonte dat de dag samen wordt begonnen. Helaas is daar deze week nog weinig van terechtgekomen doordat Hans enkele spoedoperaties heeft moeten uitvoeren. Gelukkig kan hij gewoon vanuit zijn huis opereren in zijn Virtual Reality-ruimte, anders zag hij zijn familie al helemaal niet meer. "Hans, kun jij ervoor zorgen dat de nieuwe klimaatinstellingen vandaag worden gedownload?", vraagt Elles. "Het begint alweer warmer te worden buiten en het is dus de hoogste tijd dat de instellingen worden bijgewerkt. Ik heb er zelf vandaag geen tijd voor omdat ik de hele dag de deur uit ben." Elles werkt bij een beveiligingsbedrijf en de eerste donderdag van de maand is altijd een drukke dag omdat de systemen dan nagelopen moeten worden. Daarnaast moet ze eigenlijk ook vandaag samen met Xa4 nog even snel de stad induiken om een cadeautje te kopen voor overgrootmoeder. Aanstaande zaterdag wordt ze alweer 108 en ter ere van haar verjaardag heeft het gezin besloten samen een dagje naar haar toe te gaan in het bejaardentehuis. Xa4 schenkt zichzelf nog maar eens een kop koffie in. Echt veel zin om met zijn moeder de stad in te gaan heeft hij niet, maar het is natuurlijk wel weer een mooie gelegenheid om even van dat vervelende schoolwerk af te zijn. Vandaag staat Veiligheid en Agressiebeheersing op het programma, en als hij ergens een hekel aan heeft…

Den Haag, Scholengemeenschap Watson & Crick, donderdag 2 maart 2030, 08.30 uur
Xa 4 baalt. Sinds twee maanden zit hij op de speciale school voor jongens van 12 tot 16 jaar. Zijn ouders waren ongerust door het licht verhoogde risicoprofiel dat uit Xa4s veiligheidstest kwam, en hebben hem daarom naar een speciale privéschool gestuurd voor jongens in leeftijdsgroep 12 tot 16 jaar die speciale aandacht krijgen om te voorkomen dat ze ontsporen en agressief of misdadig gedrag gaan vertonen. Dat is echter niet datgene waarvan hij baalt, want eigenlijk is het wel prettig om naar deze school te gaan. Voorzover hij weet is er het afgelopen jaar niet één keer een geweldsincident geweest. En de leraren zijn ook best aardig. Waar hij van baalt is de enorme rij die elke ochtend voor de poort staat. De scholengemeenschap is streng beveiligd; je kunt alleen binnenkomen als de irisscanner aan de poort het groene licht heeft gegeven. En dat zorgt voor nogal wat opstoppingen want sommige leerlingen proberen een nieuwe variant op het spelletje 'fop de irisscanner' te spelen – tevergeefs natuurlijk, maar het houdt de ingangscontrole wel op. Alle persoonlijke gegevens van de ingaande leerlingen worden uit de centrale databank van de Haagse school-toezichthouder gehaald, om te controleren of ze daadwerkelijk zijn toegewezen aan deze scholengemeenschap; vervolgens wordt aan de leraar doorgeseind dat de leerling – Xa4 de Vries uit de Haviklaan in Den Haag – zojuist gearriveerd is. Tegelijk wordt door het ingangspoortje de hormoonspiegel en neurohuishouding afgelezen en opgeslagen uit de mini-sensor die in het lichaam is aangebracht; Xa4 blijkt vandaag geen extra serotonine nodig te hebben. Eenmaal in het lokaal aangekomen stort hij zich met een diepe zucht op het lesmateriaal van die dag.

Den Haag, Veiligheid-eerst Centrum, donderdag 2 maart 2030, 09.30 uur
Elles is hoofd veiligheid voor het Veiligheid-eerst Centrum dat in de jaren 2010 met een startsubsidie van de overheid is opgezet. Het Veiligheid-eerst centrum beschikt over de nieuwste technologische snufjes. Het centrum kan elke camera en elke sensor in de hele stad bedienen. Zo heeft Elles zicht op alles dat er gebeurt en kan meteen ingegrepen worden als er ergens misstanden plaatsvinden. Ze is nog maar net binnen of krijgt al van haar collega Isa een statusrapport in haar handen gedrukt. "Vanmorgen vroeg is er een melding binnengekomen dat een verdachte persoon zich ophield in de buurt van het Ministerie van Europese Aangelegenheden", zegt Isa tegen Elles. "We hebben meteen alle systemen in werking gesteld en de beelden van de camera's en sensoren opgeroepen die in een straal van 100 meter rond de desbetreffende locatie opgesteld staan", meldt ze. "Ik kan u vertellen dat we binnen vijf minuten agenten ter plaatse hadden die de verdachte hebben aangehouden. Het gaat om een 30-jarige man van Nederlandse afkomst. Hij is geboren in Rotterdam, heeft twee kinderen bij twee verschillende vrouwen en is momenteel werkeloos. Zijn laatste werkgever heeft inmiddels een bericht gehad en zal de gegevens die in de bedrijfsdatabank aanwezig zijn naar ons toe te sturen. We zijn nog bezig om zijn gangen van de afgelopen weken na te gaan zodat we eventueel kunnen zien of hij zich de laatste tijd vaker bij het Ministerie heeft opgehouden. Die gegevens moeten binnen het uur beschikbaar komen als de centrale databank haar werk heeft gedaan." Elles werpt nog een blik op het statusrapport. Ze leest dat er afgelopen nacht een probleem is geweest met de beveiliging van een huis in het Schilderskwartier. De beveiliging van de huizen in die wijk is niet helemaal optimaal. De meeste inwoners hebben niet genoeg geld om geavanceerde systemen rondom en in hun huis aan te leggen. Het gebeurt daarom nog wel eens dat een kwaadwillende persoon allerlei persoonsgegevens weet te bemachtigen en daarmee heel eenvoudig de goedkope beveiliging van het huis kan doorbreken. Gelukkig is dit probleem alweer opgelost. De dader, wederom een bekende van het Veiligheid-eerst centrum, is afgelopen nacht al vrij snel in de kraag gegrepen.

Den Haag, Haviklaan 6 / Maastricht, Debyelaan 25, donderdag 2 maart 2030, 11.50 uur
Hans wordt opgeschrikt door de pieper in zijn overhemd: een spoedoperatie. Hij gaat in zijn operatieruimte aan de slag met opereren van de patiënt, Johan Vogelaar, die in het Maastrichtse ziekenhuis op de teleoperatietafel ligt. Het is een man van 24 die tegen alle seinen in een straat in Maastricht overstak waar de auto's door automatisch geleiding in dichte opeenvolging voorbijraasden. De operatie valt mee en is snel geklaard. De automatische DNA-neuro-scan toont geen bijzonderheden in Vogelaars gezondheid, aanleg of karakter, zodat de afdeling Hanbai[82] van het AZM geen gepersonaliseerde folder van behandelingen hoeft voor te bereiden voor de ontslagmap. Het systeem waarschuwt dat een hackpoging wordt gepleegd op de netwerkverbinding van de Hollanders om de operatie over te nemen, maar er is flink geïnvesteerd in de beveiliging van telechirurgieverbindingen, zodat de aanval – niveau blauw, ze worden steeds krachtiger – kan worden afgeslagen.
Wel gaat echter plotseling een paars lampje branden dat een treffer in de DNA-databank van gezochte personen signaleert. Het betreft geen volle treffer: het Y-chromosoom van Johan Vogelaar komt overeen met dat van het profiel van een vermoedelijke pleger van een aanslag uit 2018, maar de rest van het DNA-profiel wijkt behoorlijk af. Vogelaar is dus geen broer van de gezochte persoon, maar vermoedelijk een wat verder verwijderd mannelijk familielid. De gezochte persoon is geen ingezetene van Nederland, anders was zijn profiel wel direct aangetroffen in de forensische DNA-databank, die inmiddels bevolkingsbreed is opgezet. De melding van de partiële treffer komt binnen bij de recherche in Maastricht, die de rechter-commissaris verzoekt om een grootschalig familie-onderzoek van Vogelaar te verrichten. De r-c geeft toestemming, en de recherche verzoekt het forensisch

[82] Hanbai is een Japanse term voor Marketing. In 2030 verdringt het Japans langzamerhand het Engels als modetaal in uitdrukkingen en bedrijfsonderdelen.

instituut een DNA-stamboom te maken van Vogelaars familie tot in de achtste graad. Later zal uit navraag bij de gevonden familieleden blijken dat in de jaren 1990 een verre neef van Johan is geëmigreerd naar Guam, waarna een rechtshulpverzoek wordt ingediend bij de Guamse collega's om het DNA-profiel van deze neef op te vragen.
Hans merkt van al deze activiteiten ondertussen weinig; hij heeft wel het paarse lampje zien flikkeren, maar hij heeft zich na de operatie snel teruggetrokken op de bank, waar hij zich ontspant met een zaptochtje langs de vier Europese rampenzenders. Als hij overschakelt op Disaster Channel Asia ziet hij een documentaire over de traumatische bio-aanval op Singapore in 2024, die bij bijna een derde van de bevolking hersenschade aanrichtte. Hij maakt een aantekening in gedachten dat hij Xa4 eens moet suggereren om later neuromedicijnen te gaan studeren. De overal sinds 2024 opgerichte afdelingen preventieve neurogenetica kunnen ook in de toekomst wel slimme, goed opgeleide medici gebruiken. Hij belt zijn zus die werkt bij een arbeidsbureau dat is gespecialiseerd in hoogopgeleide twintigers die niet aan de bak kunnen komen omdat veel 70-plussers weigeren met pensioen te gaan zolang de AOW niet op het oude niveau is teruggebracht. 'Dag Karin, met Hans' (gek, denkt hij, hoe je je naam blijft zeggen terwijl persoonsidentificatie bij telecommunicatie al sinds jaren niet meer uitgezet kan worden, en je meestal toch gelijk in beeld komt op het huisscherm bij wie je belt). 'Zeg, ik zat te denken, Xa4 moet volgend jaar een profiel gaan kiezen, en ik vroeg me af welke sector tegenwoordig het meeste perspectief biedt.' 'Hm, ik denk veiligheid of NBIC[83], als ik het zo zie. Hoezo dat?' 'Nou, ik zag net een documentaire over Bio/Sing '24, en ik bedacht hoe belangrijk het toch is dat we meer weten hoe we het neurosysteem kunnen beveiligen tegen een bio-aanval. Dus ik denk – wat zei je? (...) Hm, dan was het zeker een hacker die ons afluistert. Belachelijk dat ze m'n netwerk alleen goed beveiligen als ik aan het teleopereren ben. Maar goed, waar was ik? Dus ik denk...'

Den Haag, Spui, 2 maart 2030, 14.30 uur
Xa4 haast zich in de richting van het Spui. Hij heeft om half drie met zijn moeder afgesproken zodat ze samen een cadeautje voor overgrootmoeder kunnen kopen. In de verte ziet hij haar al staan. "Mama!", roept hij terwijl hij snel naar de elektronicawinkel toeloopt waarvoor ze staat te wachten. Eenmaal binnen is de keuze snel gemaakt. Overgrootmoeder krijgt een nieuw *virtual reality*-masker voor haar verjaardag omdat de oude nog stamt uit 2020 en de laatste tijd steeds vaker uitvalt tijdens haar cyberomzwervingen. Xa4 rekent het masker af met zijn geïmplanteerde betaalchip. Die heeft hij al op z'n tiende laten inbrengen zodat hij op school in de kantine meteen door kan lopen als hij zijn eten op zijn dienblad heeft liggen. Zijn gegevens worden door de winkel gekoppeld aan de RFID-chip op het masker. Dan weet de winkelier de volgende keer meteen met wie hij van doen heeft en kan hij hem – onder andere door zijn aankoopgedrag te bestuderen – beter van dienst zijn. Binnen een kwartiertje staan Elles en Xa4 weer buiten. "Zullen we nog ergens een hapje gaan eten?", vraagt Elles aan Xa4. Nog voordat Xa4 zich naar zijn moeder heeft om kunnen draaien om antwoord te geven, hoort hij haar heel hard gillen: "Houdt de dief!". In de verte ziet Xa4 een man wegrennen over het Spui met de tas van zijn moeder in zijn hand. Om hem heen wordt inmiddels door verschillende omstanders druk gebeld met de politie. Iedereen die een misdaad op heterdaad ziet gebeuren is verplicht onmiddellijk de autoriteiten in te lichten. Daarvoor is 10 jaar geleden een speciaal meldpunt ingesteld; de MeldMisdaad-lijn (MM-lijn). Gelukkig beschikt iedereen tegenwoordig over een in de kleding ingebouwd communicatieapparaatje met 1-1-2-alarmknop, zodat snel actie ondernomen kan worden. Op een subafdeling van het Veiligheid-eerst centrum wordt meteen gereageerd. Direct wordt verbinding gemaakt met de databanken van zowel de bank waar Elles haar geld gepind heeft als de winkel waar de tas en de winkel

[83] NBIC = nano-, bio- en informatietechnologie en cognitiewetenschappen, waarmee de convergentie van deze vier wetenschaps- en techniekgebieden wordt aangeduid.

waar het cadeautje dat daarin zat gekocht zijn. De RFID-chips die op de grote bankbiljetten, de tas en het masker zitten worden meteen getraceerd. Bijna onmiddellijk daarna komen op het Veiligheid-eerst centrum de eerste beelden van de dader binnen. Binnen een paar minuten is de dader door de toegesnelde politieagenten ingerekend en wordt hij meegenomen. De agenten lezen zijn RFID-chip uit. Op de chip zijn alle gegevens van de dader opgeslagen. Het is een oude bekende van het Veilig-eerst centrum: de man heeft twee jaar geleden in de gevangenis gezeten voor vergelijkbare vergrijpen en is daar voorzien van een chip die hij de rest van zijn leven bij zich zal dragen.

Den Haag, Virtual Reality Entertainmentcentrum, donderdag 2 maart 2030, 20.45 uur
Xa4 is een fervent gamer en elke week gaat hij tenminste één keer naar het *Virtual Reality Entertainmentcentrum* om daar eens lekker stoom af te blazen. Vorige week verbeeldde hij zich een smokkelaar te zijn die moest proberen uit de handen van het Internationale Misdaadbestrijdingteam te blijven. Wat het deze week zal worden? Xa4 heeft nog geen idee. Gamers worden uitgebreid gecontroleerd door het centrum. Xa4 moet zich met naam en toenaam melden en zijn handpalm op de scanner leggen. Onmiddellijk verschijnt bij de medewerker van het centrum Xa4's profiel op het scherm. "Goedenavond Xa4 de Vries", zegt de medewerker, "Je weet dat alle gegevens van het spel dat je vanavond gaat spelen opgeslagen zullen worden?" Xa4 knikt instemmend naar de medewerker. Hij is inmiddels al zo vaak te gast geweest dat hij de procedure wel kan dromen. Het persoonlijke profiel van de speler wordt gekoppeld aan het spel dat je die avond gaat spelen. Die gegevens worden vervolgens weer opgeslagen in een centrale databank die geraadpleegd mag worden door opsporingsambtenaren. Zo is onlangs nog een verkrachtingszaak opgelost. De politie had namelijk een profiel van de dader kunnen vaststellen en is aan de hand daarvan gaan zoeken naar vergelijkbare spelsituaties in de databank van het *Virtual Reality Entertainmentcentrum*. "Geen enkel probleem", zegt Xa4. De autorisatie is snel geregeld en Xa4 spoedt zich naar zijn toegewezen *VR*-kamer. Heerlijk even ongestoord een paar uurtjes gamen, denkt hij, terwijl hij zijn masker opzet.

1. Een privacyscenario

Dramatis Personae

- Theo Vriezen (42), beveiligingsbeambte
- Jan Houtzager-Vriezen (41), geneticus, getrouwd met Theo
- Hel1 (15), dochter van Theo en Jan

Den Haag, Duivelandsestraat 18, donderdag 2 maart 2030, 05.30 uur
Geeuwend stapt Jan zijn werkcabine binnen, een pak drinkontbijt nog in de handen. Zijn vergadering met de internationale werkgroep *Behavioural DNA* komt zometeen bij elkaar. Afstand is inmiddels geen factor van betekenis meer, met de nieuwste generatie Virtual Reality-cabines, maar ze hebben helaas nog niets uitgevonden om de tijdsverschillen de wereld uit te helpen. De Aziaten zijn in de meerderheid en bepalen dus het tijdstip van vergadering. Jan trekt zijn sensor-handschoen aan en vraagt de cabine om verbinding met Kuala Lumpur. De vergaderzaal vult zich langzaam; Jan gaat snel de reeds aanwezigen langs om even handen te schudden en zich voor te stellen aan de nieuwe collega uit Taiwan, die onlangs een briljante ontdekking heeft gedaan door een combinatie van 28 genen te vinden die gezamenlijk verantwoordelijk zijn voor 60% van de meest voorkomende vorm van aanleg voor avontuurlijkheid. Naast hem wordt gevloekt, wanneer Jan zijn koffiemachine vraagt om een stevige bak; hij brengt per ongeluk de koffiemachine van collega Jameson in Minnesota in de war – de *virtual-reality*verbindingen interfereren soms op vreemde manieren met de spraak- en stemherkenningsoftware van de wat oudere koffieapparaten.

Den Haag, Duivelandsestraat 18, donderdag 2 maart 2030, 08.30 uur
Hel1 baalt. Sinds twee jaar zit zij op een e-school, omdat haar ouders het niet veilig genoeg vonden haar naar de plaatselijke scholengemeenschap te sturen omdat ze dan door een onveilige buurt zou moeten fietsen. Ze was veel liever naar een echte school gegaan waar ze echte mensen kon ontmoeten. Maar ja, groot voordeel is dat zij nu zelf kan bepalen wanneer en in welk tempo ze het lesmateriaal doorneemt. Daardoor blijft er weer meer tijd over om met haar vrienden te praten in de *virtual chat community*. Eerst maar eens even inloggen. Het systeem herkent Hel1 onmiddellijk als een 15-jarig meisje dat het derdejaars lesprogramma van de e-school volgt en weet welke modules ze momenteel aan het volgen is. Meer weet het systeem niet van Hel1, omdat dat niet nodig is om het onderwijs te kunnen volgen. Natuurlijk heeft zij voldoende mogelijkheden om met de leraren te communiceren in het virtuele klaslokaal. Het onderwijsinstituut mag de gegevens die daarbij ontstaan niet opslaan om te controleren of Hel1 Houtzager wel daadwerkelijk het verplichte lesprogramma volgt. Toch zal ze niet onder de school uit kunnen komen: de gegevens worden namelijk wel lokaal opgeslagen en kunnen aan het einde van de dag door de ouders gecontroleerd worden, zodat zij kunnen toezien op de inzet en leerprestaties van hun dochter. Met een diepe zucht stort Hel1 zich op de eerste lesmodule van die dag: Veiligheid en Zorg, bwèh...

Den Haag, wijk 1, donderdag 2 maart 2030, 09.30 uur
Theo is hoofd veiligheidscontrole van de gemeente, bij de afdeling die toezicht houdt op de particuliere beveiligingssector. De sector floreert sinds de jaren 2020 door de toenemende vraag om de beveiliging van de hekwerkwijken die in de loop der jaren in Den Haag zijn ontstaan. Deze wijken zijn virtueel afgeschermd van de onveilige gebieden die de gemeente niet onder controle heeft kunnen krijgen. Vandaag brengt Theo een bezoek aan gemeenschapswijk 1, dat beveiligd wordt door Veilig Thuis, een semi-privaat beveiligingsbedrijf dat beschikt over de nieuwste technologische snufjes. Het duurt wel even voordat hij de toegangsstraat naar de wijk kan binnenlopen, omdat zelfs de gemeentelijke veiligheidsbeambten eerst aan een strenge *screening* worden onderworpen alvorens zij de wijk binnenmogen. Een

oudere dame, een inwoonster van gemeenschapswijk 1, staat ook aan de poort als Theo net binnen wil gaan. "Goedenmorgen mevrouw", zegt Theo. Hij kent de mensen in de wijken niet bij naam omdat de inwoners bij het systeem niet 'bekend' zijn. "Wilt u uw pas goed dicht bij de scanner houden mevrouw?", vraagt Theo. "Het systeem heeft vanmorgen wat problemen gehad en had wat moeite de passen van al te grote afstand te lezen." De oude dame houdt haar pas voor het scanapparaat en nadat het systeem heeft bevestigd dat deze dame een inwoner van gemeenschapswijk 1 is, gaat de poort vanzelf open. Tegelijk met de veiligheid wordt ook de privacy van de inwoners gegarandeerd doordat iedere inwoner de beschikking over een eigen schild heeft dat rondom zijn woning geactiveerd kan worden. Slechts in zeer bepaalde gevallen mag dat schild door de beveiligers gedeactiveerd worden. De hekwerkwijk is erop gericht om ongewenste gasten buiten te houden. Alleen in die gevallen dat er sprake is van een ongenode gast, mag het beveiligingsbedrijf de systemen aanzetten die de schilden buiten werking stelt, zodat eventuele indringers snel en efficiënt opgespoord kunnen worden.

Den Haag, Spui, donderdag 2 maart 2030, 15.00 uur
Hel1 heeft vandaag met haar vader Jan afgesproken de stad in te gaan. Ze zou eigenlijk veel liever met haar vriendinnen gaan winkelen, denkt ze, terwijl ze naast haar vader over het Spui loopt. "Ik moet eerst nog heel even naar de bank om geld te halen", zegt Jan tegen Hel1. Jan betaalt nog steeds met contant geld, ook al is het soms wat lastig omdat je eerst naar de bank moet gaan voordat je kunt gaan winkelen. Eenmaal binnen, blijkt het niet al te druk te zijn. Hel1 slaakt een zucht van verlichting. "Pap, ik vind het toch wel heel ouderwets dat je nog steeds met contant geld betaalt. Het is toch veel makkelijker om gewoon een betaalchipje te gebruiken!" "Hel1", verzucht Jan, "hoe vaak moet ik je nu nog uitleggen dat ik het veel prettiger vind om met contant geld te betalen? Ik…". Jan is niet meer in staat om zijn zin af te maken. Twee gemaskerde mannen houden een medewerkster van de bank onder schot. Ze willen geld. En snel. Gelukkig zijn de mannen weer snel vertrokken. De politieagenten zijn direct ter plaatse dankzij het stille alarm van de bank. De agenten vragen Jan en Hel1 een beschrijving te geven van de daders. Vader en dochter kunnen het niet eens worden. Volgens Hel1 droegen de daders camouflagepakken, precies zoals die van de soldaten vroeger. Jan denkt echter dat de mannen beiden in het zwart gehuld waren. "Het geeft niet meneer", zegt een van de politieagenten, "vermoedelijk maakten de daders gebruik van kameleonkleding. Het is niet van heel groot belang dat u weet wat voor kleur de kleding was omdat daar toch geen definitief uitsluitsel over te geven is. En ze zullen inmiddels toch al wel een paar keer van kledingkleur gewisseld hebben. We kunnen de daders wel op een andere manier achterhalen." De bank beschikt over een eigen gesloten camerasysteem. De beelden mogen echter niet langer dan één dag opgeslagen worden. Maar in een geval als nu waarin er een misdrijf gepleegd is, heeft de overheid de bevoegdheid de gegevens op te vragen en te bewaren zolang dat voor het onderzoek nodig is. Het heeft meestal wel wat voeten in de aarde en er moet uiteraard snel gereageerd worden omdat anders het risico wordt gelopen dat de beelden alweer gewist zijn.

Den Haag, Duivelandsestraat 18, donderdag 2 maart 2030, 12.55 uur
Jan stapt na een broodnodig ochtenddutje weer zijn werkcabine in om even de toestand op zijn werk – het laboratorium in Dronten – te bekijken en te overleggen met collega Floris over een mogelijke ontdekking die de laatste zegt te hebben gedaan.
'Ha die Floris, alles goed? Zeg het 's, wat heb je nu weer gevonden?' 'Ik weet het niet zeker, maar ik denk dat ik wat een genenconstellatie heb gevonden voor impulsiviteit. Ik was een groot bestand aan het analyseren van mensen met aanleg voor manisch-depressiviteit, en toen ik de deelverzameling door de computer haalde van de patiënten die tijdens hun manische periode minstens vier impulsaankopen hadden gedaan, vond de computer een statistisch significant verband tussen zestien genotypen op vier verschillende chromosomen. 't Lijkt spannend en veelbelovend.

Maar eh, wat denk je, moet ik het nou eerst aan de ethische commissie voorleggen of zullen wij zelf er een paar dagen mee stoeien?'
Jan denkt na. 'Moeilijk punt. Je weet dat we niet aanleg voor gedragskenmerken mogen bestuderen als die niet direct medische relevantie hebben. Maar goed, voor bestrijding van manisch-depressiviteit kan het zeker zinvol zijn er 's naar te kijken. Alleen vrees ik dat als er iets uitkomt, ik de zoveelste kamervragen van Eindelijk Rechts al hoor: "Kan de minister aangeven of ook onderzocht is of er een verband bestaat tussen impulsiviteit en geweldsmisdrijven? Denkt u dat het mogelijk is impulsiviteit van jongens met onschadelijke medicijnen te onderdrukken? En wilt u onderzoek daarnaar stimuleren?" Terwijl we er als wetenschappers in het Manifest van Toronto juist voor gekozen hebben om uit die hele discussie te blijven over genetisch-gestuurde misdaad.'
'Ja', zegt Floris, 'dat weet ik wel, maar helemaal eraan ontkomen kunnen we toch niet. Hendriks, je weet wel, die op de XXY-afdeling zit, moest vorige week op bevel van een rechter-commissaris het DNA onderzoeken van iemand die onverklaarbaar gewelddadige woedeaanvallen had. Die had duidelijk een genetisch bepaalde abnormale hormoonhuishouding, dat zag Hendriks meteen. Kan hij weer gaan opdraven als getuige-deskundige.'
'Ik benijd hem niet. Maar als je 't goed beschouwt, valt het wel mee toch. Sinds ze die strikte scheiding hebben geformaliseerd tussen de forensische instituten en de medische onderzoekslaboratoria en geïnvesteerd hebben in uitbreiding van de forensische onderzoekers, hoeven wij niet meer te helpen die achterstand in DNA-profilering bij justitie weg te werken. Weet je nog, al die dilemma's waar we toen tegenaan liepen? Vind je een profiel dat veel lijkt op het misdaadspoor-profiel, maar niet helemaal – het is een broer, dat voel je op je klompen aan, maar je mag het niet doorgeven omdat – hallo, ben je daar nog?'
Jan zucht als de verbinding wegvalt – de zoveelste verstikkingsaanval op zijn thuiscentrale deze week. Zijn netwerkverbindingen zijn prima beveiligd tegen hackers en afluisteraars, maar tegen *denial-of-service*-aanvallen doen ze maar weinig. Zodra de centrale extra capaciteit heeft ingehuurd, flitst de verbinding weer aan. 'Goed, waar was ik ook weer? O ja, die goede oude tijd.'

Den Haag, Super Soul Member Club, donderdag 2 maart 2030, 23.00 uur
Hel1 is er helemaal klaar voor. Heerlijk een nachtje feesten in de vermaarde *Super Soul Member Club*. Terwijl ze voor de ingang staat te wachten denkt ze nog even aan die leuke jongen die ze hier twee weken geleden heeft ontmoet. Misschien is hij er ook wel vanavond… De club kent een strenge ingangscontrole. Iedereen die naar binnen wil zal zich moeten onderwerpen aan een profileringcontrole. De club mag niet de identiteiten van mensen achterhalen en registreren en daarom werkt ze op basis van profilering zodat risicovolle personen aan de ingang geweigerd kunnen worden. Voordat Hel1 naar binnen mag wordt ze dus aan een uitgebreid onderzoek onderworpen. Met behulp van sensoren en meetapparatuur worden haar biochemische niveaus gemeten. Als het systeem aangeeft dat het in orde is, mag ze doorlopen en kan het feesten beginnen. De uitkomsten van het onderzoek worden direct gewist. Bij de bar ziet Hel1 haar vriendinnen al staan. De dames bestellen snel een drankje en besluiten direct de dansvloer op te gaan. Na nog geen half uurtje heerlijk te hebben gedanst, ontstaat er enige commotie in de club. Een team politieagenten heeft zich aan de ingang gemeld met scanapparatuur. Vorige week heeft namelijk in één van de donkere kamers van de club een verkrachting plaatsgevonden en de politie heeft besloten vandaag alle mannelijke bezoekers te onderzoeken om te zien of de dader zich onder hen bevindt. 'Hè,' zegt Hel1, 'wat een gedoe, ik was net toe aan een paar uurtjes ongestoord dansen. Waarom hebben ze hier nou ook geen identificatieplicht met cameratoezicht?' Ze trekt haar woorden echter snel terug als ze bedenkt dat haar vaders nu ook nooit te weten komen dat ze vorige week door de Club geweigerd was omdat ze te veel chemodrugs had geslikt...

Literatuur

ACLU 2004
ACLU, *Naked Data: How The U.S. Ignored International Concerns and Pushed for Radio Chips In Passports Without Security*, ACLU, 2004, <http://www.aclu.org/Privacy/Privacy.cfm?ID=17078&c=130#FileAttach>.

Collings & Avouris 2000
P. Collins and P. Avouris, 'Nanotubes for electronics', *Scientific American* 2000, p. 62-69.

Dershowitz 2002
Alan M. Dershowitz, *Why Terrorism Works. Understanding the Threat, Responding to the Challenge*, New Haven & London: Yale UP 2002.

Fiedler & Reynolds 1994
Frederick A. Fiedler & Glenn H. Reynolds, 'Legal Problems of Nanotechnology: An Overview', 3 *S.Cal.Interdisciplinary.L.J.*, p. 593-629, <http://discuss.foresight.org/~peterson/FiedlerReynolds.html>.

Hoogenboom 2000
A.B. Hoogenboom, *Privatisering van toezicht en opsporing*, Lelystad: Vermande 2000.

Hornung 2004
Gerrit Hornung, *Biometric Identity Cards: Technical, Legal, and Policy Issues*, in Paulus S. et al. (ed.), *ISSE 2004 Securing Electronic Business Processes*, Wiesbaden: Vieweg 2004, p. 48-57.

ISTAG 2001
IST Advisory Group, K. Ducatel e.a., *Scenarios for Ambient Intelligence in 2010, Final Report*, Sevilla 2001, <ftp://ftp.cordis.lu/pub/ist/docs/istagscenarios2010.pdf>.

Jobling & Gill 2004
Mark A. Jobling & Peter Gill, 'Encoded Evidence: DNA in Forensic Analysis', *Nature Reviews 5*, October 2004, p. 739-751 (748).

Koops 1998
B.J. Koops, *The Crypto Controversy. A Key Conflict in the Information Society*, diss. Tilburg, 301 p. Kluwer Law International, The Hague etc. 1998.

Koops 2003
B.J. Koops, 'Het Cyber-crimeverdrag, de Nederlandse strafwetgeving en de (computer)criminalisering van de maatschappij', *Computerrecht* 2003 nr. 2, p. 115-123.

Koops & Prins 2003
B.J. Koops & J.E.J. Prins, 'De toenemende strafbaarstelling van technische hulpmiddelen: over intenties, bestemmingen en instrumentele wetgeving', in: M.S. Groenhuijsen & J.B.H.M. Simmelink (red.), *Glijdende schalen* (de Hullu-bundel), Nijmegen: Wolf Legal Publishers 2003, p. 341-386.

Koops, Van Schooten & Prinsen 2004
Bert-Jaap Koops, Hanneke van Schooten & Merel Prinsen, *Recht naar binnen kijken. Een toekomstverkenning van huisrecht, lichamelijke integriteit en nieuwe opsporingstechnieken*, Den Haag: Sdu 2004, ITeR-reeks deel 70, 221 p.

Mulhall 2002
Douglas Mulhall, *Our Molecular Future: How Nanotechnology, Robotics, Genetics, and Artificial Intelligence Will Transform Our World*, Amherst, NY: Prometheus Books 2002.

Reynolds 2001
Glenn Harlan Reynolds, 'Environmental Regulation of Nanotechnology: Some Preliminary Obeservations', *Environmental Law Review* 2001/6, p. 10681-8.

The Royal Society & The Royal Academy of Engineering 2004
The Royal Society & The Royal Academy of Engineering, *Nanoscience and nanotechnologies: opportunities and uncertainties*, July 2004, <http://www.nanotec.org.uk/finalReport.htm>.

SCR 2004
Sociaal en Cultureel Planbureau, In het zicht van de toekomst: Sociaal en Cultureel Rapport 2004, SCP 25 oktober 2004, beschikbaar op <http://www.scp.nl/publicaties/boeken/9037701590.shtml>.

Stevens, Koops & Wiemans 2004
L. Stevens, B.J. Koops & P. Wiemans, 'Een strafvorderlijke gegevensvergaring nieuwe stijl', *Nederlands Juristenblad* 2004/32, p. 1680-1686.

Stuurman 2003
C. Stuurman, 'Mr. Robot, I presume...', *JAVI* 2003/6, p. 213-4.

TAB 2003
Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag, *Zusammenfassung des TAB-Arbeitsberichtes Nr. 92*, November 2003, <http://www.tab.fzk.de/de/projekt/zusammenfassung/ab92.htm>.

Warwick 2002
Kevin Warwick, 'Identity and Privacy Issues raised by Biomedical Implants', *IPTS Report* 67, 2002, <http://www.jrc.es/pages/iptsreport/vol67/english/IPT5E676.html>.

Bijlage I. Verslagen van de expert-vraaggespreken

Vraaggesprek met Ybo Buruma

Rachel Poels, 9 december 2004

Ybo Buruma is hoogleraar straf- en strafprocesrecht aan de Radboud Universiteit Nijmegen.

Veiligheid

Veiligheid is een diffuus begrip en daardoor moeilijk te definiëren. Voor de een gaat het om hangjongeren en de ander associeert veiligheid met de jongen die hem op straat heeft *geript* en weer een ander gaat het om terrorisme en Osama Bin Laden. Ybo Buruma ziet veiligheid in drie dimensies: "Eén: wat ik nu maar noem de veiligheid van de risicosamenleving. En dan gaat het om zaken als de veiligheid van voedsel en waren. Al die dingen die vanuit een normaal werkend systeem kunnen ontploffen. Twee is de externe veiligheid, de *security*. Daarbij kun je denken aan bedreigingen vanuit het buitenland. Het derde is eigenlijk een beetje hybride. De binnenlandse veiligheid en justitiegerichte veiligheid. Daarbij gaat het om mensen die bij ons horen – in ons systeem horen – maar die zich om wat voor reden dan ook niet helemaal aan de regels houden. Niet goed bedoelend falen, maar opzettelijk de fout ingaan. Als je die driedeling aanhoudt dan denk ik dat veiligheid is dat je op alle drie die fronten probeert de negatieve dingen tegen te gaan. Dat is nu zo en dat zal in 2030 ook zo zijn."

Het verschil tussen de situatie zoals die nu is en de situatie zoals die in 2030 vermoedelijk zal zijn, heeft volgens Buruma te maken met de soort bedreigingen. Volgens hem zullen die anders zijn dan nu het geval is. "Ik kan me voorstellen dat we in 2030 – met betrekking tot de eerste pijler – veel meer nadruk leggen op de veiligheid van communicatie-infrastructuren. En misschien wel minder op de veiligheid van onze treinen omdat we weten dat de veiligheid van de treinen ook bepaald wordt door het falen van de communicatie-infrastructuren. En zo kan ik me met betrekking tot de tweede pijler voorstellen dat de nadruk dan bijvoorbeeld ligt op uit China afkomstige terroristen. Nu ligt de nadruk heel erg op terrorisme uit het Midden-Oosten. De wereld gaat natuurlijk verschrikkelijk veranderen als Iran in 2007 bijna zeker een atoombom heeft. Dat is niet meer tegen te houden. Het is heel spannend of Israël Iran dan gaat aanvallen en wat Amerika vervolgens gaat doen. Als je dat perspectief erbij gaat halen, dan is het dus zeker dat ook in de tweede dimensie van veiligheid enorme veranderingen zullen komen. Die derde dimensie is het alleringewikkeldst. Ik ga er toch nog altijd vanuit dat mensen misdaden plegen vanuit hartstochten of om er beter van te worden. Ik kan me voorstellen dat als onze samenleving op het eerste front steeds meer beveiligd is er dus meer geweldsdelicten moeten worden gepleegd." Buruma denkt daarbij bijvoorbeeld aan het stelen van een auto. Dat zal niet meer zo gemakkelijk zijn als momenteel het geval is. Auto's zullen op een meer geavanceerde manier beveiligd zijn waardoor je als dief niet meer een auto kunt starten door de draadjes aan elkaar te verbinden zoals je in Hollywoodfilms wel ziet. Juist door deze technologische ontwikkelingen zullen er dus meer gegevens afgedwongen moeten worden bij het slachtoffer zoals de code die toegang geeft tot de auto.

Volgens Buruma zal de vergrijzing ook gevolgen hebben voor de veiligheid. Hij ziet die gevolgen tweeledig. Ten eerste verwacht hij dat mensen zich steeds meer zullen terugtrekken in hun eigen woongemeenschappen en ten tweede verwacht hij dat zij zich af zullen sluiten van andere groeperingen binnen de samenleving. "Mensen zullen zich meer terugtrekken in hun eigen huizen; daarbij zullen ze gezamenlijk privé-bewaking inhuren en hekken om hun zogenaamde *gated communities* plaatsen. Maar ook in het domein dat hun vertrouwd is. Dat hoort bij mensen die ouder worden; die gaan terug naar hun *roots*. Ze zullen bijvoorbeeld wel gaan surfen op het web, maar dan zullen ze surfen op dingen waar ze andere oudjes kunnen tegenkomen. Ik denk dat ze steeds minder contact hebben met anderen en dat er wat dat betreft steeds sterkere verdelingen binnen de samenleving gaat ontstaan tussen 'machtige oude rijken' en 'nieuwe jonge – ook allochtone – mensen'." Buruma verwacht dat het effect van die terugtrekkende beweging in eigen groepen zal zijn dat jonge allochtonen neergezet zullen blijven worden als een angstwekkende groepering. Hij ziet echter tegelijkertijd een mogelijk positieve invloed wat betreft jonge allochtone meisjes. Zij zullen veelal laag opgeleid zijn en daardoor terecht komen in verzorgende beroepen. "Dat is iets waardoor er toch wel een contact kan ontstaan. Voor hun broertjes zijn de oude rijken bang. Je kan je dus voorstellen dat die verzorging juist een enorme warmte en herstel van samengaan teweeg brengt. Dan kan het weer heel erg de goede kant opgaan. Dat die lullige vijftigers van dat moment worden gecorrigeerd door hun zeventigjarige ouders die zo'n ontzettende aardige Fatima aan hun bed hebben staan. Ook dat soort mechanismen moet je heel goed voor ogen hebben; dat kan namelijk heel goed gebeuren."

Buruma voorziet voor 2030, zoals gezegd, een sterkere scheiding tussen groepen burgers in de maatschappij. Mensen zullen zich steeds verder terugtrekken in hun eigen kleine kring, meent hij. "Er gaat een neiging komen dat er sprake is van meer *bonding* en minder *bridging*. Er komt meer vertrouwen in de eigen kring. Mensen raken meer op elkaar betrokken. Ik verbeeld me dat dat nu ook gaande is. De prijs van meer *bonding* is dat er minder sprake is van *bridging*. *Bridging* komt erop neer dat je juist de hand toereikt aan mensen die jou minder bekend zijn: gratis bloed geven aan de bloedbank is een voorbeeld van bridging; het t-shirt met het logo van jouw universiteit aantrekken is bonding. Een wereld zonder '*kindness of strangers*' is een wereld van kleine eilandjes. Heel klein en lokaal. Ook in de niet-*gated communities* – de mensen die het niet kunnen betalen om in *gated*

communities te wonen – krijg je meer *bonding*, een situatie als in de jaren 30. Dan zijn er wel wat vaders die samen door de buurt gaan lopen. Mensen die wel wat voor elkaar willen gaan zorgen, mits ze elkaar kennen. Als er geen overheid is die wat doet, dan moet je wel samenwerken. Dat dringt zich naar voren; zelfs in zeer criminele wijken zie je dat ze elkaar wel vaak wat helpen. Ik kan me wat dat betreft voorstellen dat het vertrouwen wel wat groter wordt tussen mensen onderling. Maar dan heel gelokaliseerd, heel kleinschalig. En dat *bridging* tussen de verschillende groepen, dat idee dat je allemaal deel uitmaakt van één kosmopolis, steeds moeilijker wordt. Het Internet doet daar niet aan af, want mensen zoeken – zoals Cass Sunstein al heeft beschreven (Republic.com) – vooral geestverwanten en bijna-bekenden: het Internet draagt hooguit bij aan deterritorialisering van de groepsvorming en dat zal de lokale groepsvorming bemoeilijken"

De rol van de overheid in een veiligheidsmaatschappij

De rol van Europa zal exploderen in gewicht en daardoor zal de overheid op een nog grotere afstand van de burger komen te staan, meent Buruma. "Ik zie wat dat betreft een positie voor de overheid ontstaan waarbij het erop lijkt zoals het al in de Verenigde Staten is. Dus dat er een paar *talking heads* zijn waar je heel krachtige emoties bij voelt die leidende rollen innemen, maar die voor een heel groot deel op pure emotionele geladen issues zullen leiden. Daarnaast zal het strafrecht een krachtige eigen stempel gaan drukken. Iedereen wil veiligheid." Volgens Buruma zullen er samenlevingsverbanden ontstaan die een aantal taken die nu bij de overheid liggen, zullen overnemen zoals de verzorging of voorzieningen voor werkelozen. "Er zal een privatisering komen van zaken die nu onder de sociale welvaartsstaat vallen. Er zullen wel intermediaire instituten komen die ook redelijk werken. Dat betekent dat de overheid dus wat dat betreft een beetje op afstand komt te staan. Dit is tweeledig: aan de ene kant snappen ze er geen zak van wat de mensen bezig houdt en aan de andere kant zullen ze er ook minder over te zeggen hebben. Het zal me niet verbazen als deze tijden van de dikke stroop – ofwel de tijden waarin de managers het allemaal voor het zeggen hebben – dat die geleidelijk aan toch weer vervangen gaan worden door een tijd waarin professionals het weer meer voor het zeggen gaan hebben. Mensen die ook iets kunnen. Ik sluit niet uit dat er wat dat betreft toch iets komt vanuit de samenleving zelf. Dat men de dokter zijn of haar doktersdingen laat doen in plaats van dat het verzekeringsbedrijf dat bepaalt. En dat dit bij een politieagent ook zo is. Toch is dit een van de onderwerpen – de politie – waarvan ik denk dat de overheid dat wel voor een deel in eigen handen zal houden. We gaan naar een enorme privatisering van de politie, dat is al gaande. Alles in de eerste pijler dat wordt allemaal privé-politie. Ik geloof er niets van dat we nog lang inspecteurs van de warenwet zullen hebben die van de overheid zijn. Dat worden een soort Buma-Stemra's. Dat gaat allemaal vanuit de belanghebbers: Albert Heijn zal bijvoorbeeld eisen gaan stellen aan voedsel om allerlei anderen uit de markt te kunnen persen. De hoofdrolspelers in het private veld gaan zelf de handhavingsystemen hanteren zodat zij de kneuzen eruit kunnen zwiepen en daarmee hun eigen positie kunnen versterken. Dat zie je nu al bij de particuliere beveiligers; die willen zelf gedragscodes met strenge handhaving om erop toe te zien dat de beveiliger wel netjes optreedt. Zodat allerlei vrije jongens op die manier buiten de deur gehouden worden."

Privacy

Buruma denkt dat ook het privacybegrip van inhoud zal gaan veranderen in de richting van 2030. "Ik denk dat privacy dan preciezer gedefinieerd is. Dat het beperkter wordt opgevat dan het nu wel heel bodemloze begrip dat het is. We zullen meer teruggaan naar de kernzaken. Het eigen huis, het gezin. Ik denk dat we, daar waar het om privacy van informatie gaat, veel strenger gaan worden met betrekking tot datgene wat we als privacy zien." Buruma verwacht dat mensen een weerwoord zullen krijgen als het gaat om de opgeslagen persoonsgegevens. Op het moment dat die gegevens gebruikt worden, krijgen mensen dan de gelegenheid tegen eventuele onjuistheden te ageren. "Privacy zal veel meer met hoor- en wederhoor worden gedefinieerd daar waar het om gegevens gaat. Er zullen ook vast een aantal schandalen komen over verkeerd opgeslagen en verkeerd geanalyseerde gegevens waar vervolgens consequenties aan worden verbonden die vreselijk worden gevonden. Er zullen eerst vijf huizen ten onrechte worden ingevallen op grond van verouderde gegevens zoals in de reclame van Praxis. Daarna zal er iets gebeuren dat echt erg is. Dan denk ik dat er een moment van tegensputteren moet zijn geweest waarop je gezegd hebt: 'dit is allemaal verouderd, want...' Dit zal meer ingebouwd gaan worden. Dat privacy een punt wordt van argumenten om over te spreken. Over hoe er met het virtuele beeld dat van jou bestaat wordt gehandeld in plaats van dat het een zelfstandig iets zal zijn waar dus niets mee mag. De huidige neiging dat je niets meer mag opschrijven is al zo uitgehold van binnen."

Dat instellingen verplicht zullen worden gegevens voor een (on)bepaalde tijd op te slaan, weet Buruma wel zeker. "Ik denk dat het eerder een vraag zal zijn van: in hoeverre niet? Ik acht de kans nihil dat het niet zo is. Ik denk dat je het gaat kopen namelijk. Je kunt auteursrechten op je virtuele persoonlijkheid gaan kopen. Je kunt dan gaan procederen over het illegale portretrecht van jouw virtuele persoonlijkheid. En dat je op die manier jezelf kunt verdedigen tegen ongeautoriseerde handelingen hiermee. Niets zal echt beschermd zijn als het over dit soort gegevens gaat, maar ik denk wel dat je kunt 'toeslaan'. Ik denk dat het een waanzinnige strijd gaat worden; een strijd die je nu al ziet waar het gaat om DNA-structuren. Zo zie je bijvoorbeeld in Amerika dat het bedrijf dat zich bezig houdt met het menselijk genoom alles doet om dat auteursrechtelijk te beschermen zodat iedereen die met die kennis pillen wil maken daarvoor moet dokken. Sommige pillen kunnen bijvoorbeeld niet meer gemaakt worden omdat het zo duur is om onderzoek te doen omdat onderzoekers aan die commerciële ratten van het Amerikaanse genoomonderzoek moeten betalen. Ik denk dus dat we dit kunstje gaan leren en moeten

gaan leren ten aanzien van onze eigen virtuele persoonlijkheid. En dat je daar dus jezelf in kunt gaan beschermen om te zorgen dat je daar geld voor kunt krijgen."

Ook op het gebied van de privacy verwacht Buruma invloeden van de vergrijzing. "Op allerlei manieren zal deze invloed hebben. Iemand die vergrijst zal natuurlijk in een geriatrische inrichting zitten; die heeft een privacy van drie keer nul. Aan de andere kant, wanneer het gaat om gegevens, dan weet ik het ook niet want op dit moment vinden de apothekers het al normaal dat ze via volstrekt onbeveiligde verbindingen de gegevens van hun patiënten uitwisselen. In de praktijk gaat het als ik goed geïnformeerd ben, veel minder zorgvuldig dan je zou verwachten. Dat gaat dan ook een keer mis. Daar kun je donder op zeggen. Maar op dit moment wordt ook door veel mensen gezegd: 'Who cares dat ik aan de Ritalin ben? Who cares dat de hele wereld aan de Prozac is en dan zijn we allebei gelukkig.' Of missers met het oog op de informationele privacy in de waardering de doorslag gaan geven, of dat de relativering dat doet – die er ook bij veel mensen bestaat als het bijvoorbeeld om dit soort zorg-kwesties gaat -, weet ik niet; die glazen bol is me net één slag te moeilijk."

Het strafrecht

Op zijn eigen vakgebied ziet Buruma ook enkele belangrijke veranderingen. Zo staan we volgens Buruma nu al op een overgangsmoment en zal er in 2030 wederom sprake zijn van een omslag in het strafrecht. "Op dit moment worden in het strafrecht de formaliteiten sterk gerelativeerd. Dat zal gepaard gaan met (of gecompenseerd worden door) een lichte versterking van een accusatior procesmodel waarbij je dus als verdachte wel weer wat meer gelegenheid krijgt om aannemelijk te maken dat jij het niet was. Dat jij geen opzet had. Met name in de psychische factoren zullen de eisen nog wel wat strenger worden, zodat daar nog wel een rem zit of je veroordeeld zal worden." Daarnaast verwacht Buruma dat een heel groot deel van het strafrecht zal worden afgesplitst. "Het zal hetzij worden afgesplitst doordat er dingen via bestuurlijke boetes plaatsvinden, hetzij doordat er veel meer op personen dan op daden worden gereageerd. Risicovolle personen gaan *kaltgesteld* worden zodat ze hun snode plannen niet kunnen uitvoeren. Dat gebeurt op grond van risico-analyses die ze onder andere via de computers gaan maken."

Het doorschieten van het geloof in risico-analyses ziet Buruma heel zwart in. Dat is een zekerheid; een gegeven. "We zijn al zo doorgeschoten waar het gaat om zedendelinquenten. Als je een perverse zedendelinquent bent, kom je er nooit meer uit. Die gaan nu al de *long stay* in. Je mag hopen dat je je een beetje hebt ingehouden tijdens de verkrachting. Dat je dus een gewone zedendelinquent bent. De risico-analyses gaan de kant uit van 'je vond het ook nog leuk om een bh in stukjes te knippen, dus dan ga je in de *long stay*'. Dat model zal alleen maar worden uitvergroot. Je kunt nu uit MRI-scans de verminderde hersenactiviteit bijvoorbeeld in de pre-frontale kwab bij sommige mensen waarnemen. Het is inmiddels ook al wel aannemelijk dat als er minder elektronische hersenactiviteit is dat je dan ook wat minder decorumneigingen hebt en dat je je minder geremd voelt. Dat je ook bijvoorbeeld gemakkelijker in agressieve daden vervalt. Naast dit soort cognitie-wetenschappelijke indicatoren, zijn er ook genetische, psychologische en sociologische gegevens die vrij krachtige voorspellers opleveren. Je kunt je dus voorstellen dat je op grond van verschillende kenmerken kunt vaststellen: 'dat wordt geen fijn jongetje; dat is een risico'. 'Je hebt een keer je neus op de verkeerde plek gesnoten. Het delict is minimaal, maar hij voldoet aan het risicoprofiel en daarom vinden we hem een engerd: 'die zetten we weg'. In een pure veiligheidsstaat laten we het daarbij; in een samenleving van 2030 waarin nog enig respect voor privacy bestaat, zal men zich tegen dit soort profilering kunnen verdedigen "

Met betrekking tot de laatste twee dimensies van veiligheid, het gebied van oorlog en terrorisme enerzijds en dat van de klassieke delicten zoals moord en verkrachting anderzijds, verwacht Buruma dat het een periode zo zal zijn dat mensen een heel groot geloof hechten aan de risico-analyses van psychiaters. Verdachten zullen op grond van dergelijke risico-analyses worden opgepakt. "Dat gaat op een gegeven moment fout. In het begin zal het nog wel een tijdje zo zijn dat mensen zeggen: 'dat is toch allemaal mooi en kijk eens, we hebben die persoon die zich schuldig heeft gemaakt aan een feit toch vrijgesproken want hij kon het toch allemaal niet helpen. En díé engerd hebben we in de gevangenis gestopt'. En dan gaat er een tegentendens komen. We zitten dan al in de buurt van 2030. Dan zijn er te vaak gebeurtenissen geweest waarbij bleek dat dit model faalt. Daarop zal een tweede omslagpunt volgen. Dan zullen we net in 2030 zitten en dan zijn er een aantal gebeurtenissen geweest die mensen zo zullen ontstellen omdat het Openbaar Ministerie te wild is opgetreden. Dat daar dus evidente fouten zijn gemaakt. 'Jezus, nu is het toch uit de hand gelopen'. Ik verwacht wel dat dat ongeveer in 2030 zal inzinken."

Buruma verwacht dus dat de nadruk gedurende een bepaalde tijd heel erg zal komen te liggen op de voorfase waarin preventief opgetreden kan worden. Of er echter ook zoveel aandacht zal zijn voor de nafase betwijfelt Buruma. "Ik sluit niet helemaal uit dat het systeem dat niet aankan. Het is natuurlijk normaal dat je, bij iemand die de gevangenis uitkomt, de neiging hebt om te zeggen: 'zo iemand, daar moeten we even naar kijken'. De ervaring leert een beetje dat het met al die dingen van achteraf in de gaten houden, zo vaak misgaat. Tenzij er zeer gereguleerde systemen van *parole* voor bestaan waardoor mensen terug moeten komen. Maar dat is duur. Het alternatief staat of valt het met de vraag of we nog enigszins wijkagenten hebben die met mensen praten. Als die hybride functie van agenten die zichtbaar een praatje met mensen maken, hen een beetje helpen en en passent inlichtingen krijgen, blijft bestaan – en ik ga er maar vanuit dat dat voorlopig nog wel zal gebeuren – dan zou het kunnen. Dan kun je de ex-gedetineerde op een menselijke manier in de gaten blijven houden. Maar dan zie ik niet een kwalitatief enorme verandering ten opzichte van de huidige situatie. Het kan zijn dat

er meer bijzondere voorwaarden komen; dat je een enkelband moet dragen. Dat zal wel. Het kan ook zo zijn dat er – nog veel meer dan nu – detentie buiten de muren plaatsvindt. Dan heb je het eigenlijk over dezelfde mensen, maar die dan een vorm van huisarrest hebben. Naarmate de politiefunctie meer wordt opgesplitst in ongerelateerde taken en men minder in Humint (menselijke intelligence, wijkagenten, informanten, undercovers) dan in Sigint gelooft (camera's, taps, trackers), wordt het voor ex-gedetineerden moeilijker zich te onttrekken aan het oog van de overheid, maar ook moeilijker om terug te keren in een geregeld leven. Databestanden zullen onmiddellijk aangeven dat deze *ex-con* door de sollicitatieprocedure heenkomt: dat zal hem dwingen zich terug te trekken in criminele bendes."

Voor de burger ziet Buruma ook een rol in het strafrecht en dan met name waar het gaat om de opsporing. Een algemene aangifteplicht voorziet hij echter niet. "Misschien wel in sommige beroepen. Vertrouwensartsen bijvoorbeeld en bij kindermishandeling. Dat zou met niet verbazen als dat wat meer doorzet, maar niet heel veel. Burgers hebben de neiging om hier geen gehoor aan te geven. Dat dat misschien wel moet, maar dat ze het gewoon niet doen. Ik denk vooral eigenlijk aan het meewerken met betrekking tot gegevens die zij hebben. En ook dat zit nu al in de pijplijn, dus dat is niet zo heel bijzonder." Wat betreft het opsporen van strafbare feiten maakt Buruma een onderscheid tussen gewone burgers en professionele opsporingsgerichte burgers. Hij acht de kans heel groot dat de tweede categorie sterk zal opkomen. "Ik denk zelf dat die burgers een grotere rol zullen krijgen in allerlei economische delicten. En ook in de sfeer van dat wat nu in de Algemene Plaatselijke Verordening geregeld is. Dat zou ik niet uitsluiten dat dat als het ware steeds meer geprivatiseerd wordt. De kern van het strafrecht, zaken zoals moord en doodslag, zullen nog wel heel lang in handen van de politie blijven. Daarnaast denk ik dat er wel steeds meer verplichtingen zullen zijn voor burgers om mee te werken, dus om allerlei gegevens aan te leveren, bijvoorbeeld virtuele beelden."

Het laatste woord

Op de vraag of er wellicht nog zaken zijn die hij graag aan de orde wil stellen, antwoordt Buruma: "Misschien één ding en dat is via de lijn waarmee ik begon. Maar dat is dus ook zo'n lastige. Ik ben tijdens het praten steeds bezig met het extrapoleren van de feiten die ik nu weet en tegelijkertijd waren veranderingen op het collectieve emotionele vlak in mijn woorden niet te vinden, behalve in het stuk over de verzorging. De kans is heel groot dat we een samenleving worden waarin breed gedeelde wrok en gefnuikte verwachtingen een veel groter invloed hebben dan bijvoorbeeld de stand van de techniek. Ik heb het verschil in wereldbeeld van generaties altijd een heel bijzonder iets gevonden. De generatie van 45-55, die een heel optimistisch 'wij gaan de wereld veranderen' beeld hebben gehad. Die waren altijd heel erg van 'we gaan iets doen'. Terwijl de generaties daarna niet steeds dat hoopvolle van de jonge jaren hebben meegekregen. Als je in de jaren 80 heel jong was dan kreeg je van je ouders niet het wereldbeeld mee van 'het wordt allemaal steeds beter'. Het was hooguit dat het allemaal steeds iets comfortabeler kon. Maar voor de rest was er niet veel reden om vrolijk te worden. Zo kan ik me voorstellen dat als nu de economie weer gaat zakken, er mensen komen die geen erg optimistisch wereldbeeld hebben. En wat dat betekent, daar heb ik nog niet over nagedacht. En ik weet ook niet in hoeverre het privacy- en veiligheidsbeeld dan verandert. Op het moment dat je denkt 'morgen wordt het alleen maar slechter' kun je dus twee effecten hebben. Dat je gaat sparen en je heel erg terugtrekt in je nestje. Dat zou een reactie kunnen zijn. Het kan ook zo zijn dat je in alles verwacht dat je wel genaaid zal worden. Dat het vertrouwen in andere mensen ontzettend gaat zakken. Dat zijn alweer twee verschillende scenario's uit iets dat wel eens heel invloedrijk zou kunnen zijn."

Daarnaast vraagt Buruma zich af wat de invloed van religie zou kunnen zijn voor de vormgeving van de samenleving. "Die collectieve emoties kunnen ook geweldig doorwerken als ze impliceren dat het huidige geseculariseerde tijdvak verandert in een tijdvak dat weer veel meer door religieuze noties gedomineerd wordt. Het is niet uitgesloten dat het normaal is dat we allemaal naar de grote media van Fox kijken die dan ook gewoon hier religieus zijn en dat die niet alleen meer leuke kinderprogramma's doen. Die ons iedere avond overstelpen met bijbels getinte toestanden. Hoe je het ook wendt of keert, dan weet je zeker dat er toch weer mensen zijn die die kant opgaan. Dat zou de samenleving ook enorm kunnen veranderen en beïnvloeden. En wat dat dan voor privacy en veiligheid doet? Nou voor privacy bijvoorbeeld: als het echt zo religieus wordt, dan moeten mensen nog meer gaan vertellen over hun diepste zieleroerselen. Dat wordt dan misschien wel opgenomen op band. Het is in sommige van die protestante groepen heel gebruikelijk dat je in het openbaar je zonden belijdt. Nou, en als er een bandje meeloopt, dan zal dat dus ook van invloed zijn hierop. We hebben het al een keer meegemaakt dat om deze reden werd geïnfiltreerd in zo'n religieuze groep. Het punt van die cultureel emotionele invloeden kon wel eens groter zijn dan we geneigd zijn te doen geloven met betrekking tot invloeden van de techniek."

Buruma wil nog afsluiten met een positief punt. "Ik denk dat er, in ieder geval in de periode tot 2030, meer opgedrongen zorg gaat komen. Bemoeizorg. Dat zit nu al in de lucht en dat is vanuit een privacyoogpunt dubieus. Tot op zekere hoogte heeft dat ook wel iets moois. Gezinnen waar het helemaal misgaat, want we kunnen niets. 'Sorry, handen gebonden: privacyregels'. Ik denk dat het echt gaat komen dat mensen die zitten te verkommeren – die zitten te verhongeren zelfs omdat ze niet weten hoe ze dingen moeten kopen – dat die opgedrongen hulp gaan krijgen."

Vraaggesprek met Erik Huizer

Ronald Leenes, 6 december 2004

Erik Huizer is directeur innovatie en business development bij de NOB en deeltijd-hoogleraar aan de UT en UU op het gebied van Internettoepassingen.

Veiligheid in 2030 is niet wezenlijk anders dan nu. Veiligheid is een perceptie van de burger dat hij zich zonder belemmeringen kan bewegen in de maatschappij zonder beroofd te worden of neergeschoten en dergelijke. Deze definitie is betrekkelijk constant en ook niet gewijzigd na 9/11. De perceptie van burgers is sinds de aanslagen veranderd: misschien bedreigt dit ons ook. Van de overheid wordt vervolgens verlangd de balans te herstellen. Is de balans in het streven veiligheid te herstellen doorgeslagen naar veel zwaardere maatregelen dan we zouden willen, waardoor de vrijheid weer in het gedrang komt.
Privacy is nagenoeg de inverse van veiligheid. Privacy is moeilijk in absolute termen te vatten. In regelgeving wordt een poging gewaagd. Privacy is iets dat in de beleving van burgers leeft. Iets als identificatieplicht op straat zonder concrete verdenking was 10 jaar geleden onacceptabel. Inmiddels zijn de grenzen zodanig verschoven dat het voor de burger acceptabel is. De behoefte aan privacy verschuift op basis van maatschappelijke veranderingen. Je kan vervolgens kijken naar verschillende terreinen van privacy: gegevens over gebruikers, handelswijze (activiteiten). Met betrekking tot gegevens van gebruikers zie je dat de wetgeving strikter is dan de burger noodzakelijk acht. Dat is goed want in zekere zin bescherm je deze daarmee, maar ik denk dat daar tot 2030 nog wel eens een hoop zou kunnen veranderen. Op administratief gebied zal de privacy dan veel minder zijn dan nu. Privacy met betrekking tot het volgen van activiteiten ligt veel gevoeliger. Daar voelen mensen zich veel sneller aangetast. Fouilleren op straat valt mee als dat eenmalig, enkel en niet persoonsgericht is, maar zodra dat wel het geval is zijn mensen daar bijzonder huiverig over en dat zal in 2030 ook nog wel zo zijn.
Bij **techniek** verwacht ik dat we voor een groot deel zijn teruggeworpen op ICT en dan met name op de C. Ik denk dat we wereldwijd het besef krijgen dat de energievoorraden niet onuitputtelijk zijn. Dat gaat in vlagen. In de zeventiger jaren is er veel gedaan aan besparing, nu veel minder. En ook in ontwikkelingslanden, zoals China, wil iedereen een auto hebben. Dat legt een groot beslag op energiebronnen, vooral olie. In 2030 moeten er niet alleen alternatieven zijn, en dat zijn er niet veel. Mensen moeten ook naar andere wegen zoeken om hiermee om te gaan. Beperken van mobiliteit is een belangrijke mogelijkheid. Er lijkt een recht van mobiliteit te zijn ontstaan en ook een wet van behoud van mobiliteit: wie minder voor zijn werk reist, gaat meer privé rijden. De overheid zal maatregelen moeten nemen. Prijzen zullen enorm omhoog gaan voor vliegen en autorijden. Voor communicatie zullen we daardoor steeds meer afhankelijk worden van ICT. Tegen 2030 hoop ik dat we glasvezel hebben liggen naar elk huis, dus op zich is dat geen probleem. We moeten dan met elkaar gesprekken kunnen opzetten waarbij we elkaar met behulp van de beschikbare technologie diep in de ogen kunnen kijken. Die ontwikkeling strekt zich uit van het vergaderen via teleconferencen, telewerken tot consulten van medici en dergelijke waardoor een bezoek aan het ziekenhuis niet nodig is. Ook voor beveiliging is dit een optie. Je hoeft niet met een auto rond te rijden, je kunt ook camera's plaatsen. Ik voorzie glasvel tot aan de deur en draadloos binnenshuis. Dat kan anders zijn als de militaire communicatiebanden worden vrijgegeven. Dat zou de benodigde bandbreedte opleveren om overal draadloze breedbandcommunicatie mogelijk te maken, maar ik zie dit politiek niet gebeuren. 80% van de vergeven banden wordt niet of nauwelijks gebruikt (recent rapport, metingen in Brussel).
Ik verwacht ook dat mensen dingen die ze thuis doen, kijken, luisteren, naast bellen en SMSen, steeds meer onderweg zullen willen doen. Je ziet een convergentie van verschillende apparaten. De iPod heeft de CD overbodig gemaakt. De iPod kan overbodig worden als je de data gewoon uit de lucht kan halen. De opslag van data kan veel goedkoper en batterijvriendelijker elders plaatsvinden, dus waarom zou je alle data met je meeslepen. Op mobiel gebied zal er een grote integratie plaatsvinden.
Internet versterkt dingen die er al lang zijn. Dingen die door Internet naar voren komen en waarvan mensen zeggen dat is slecht aan Internet, denk aan kinderporno, zijn nooit zaken die specifiek door Internet zijn ontstaan. Ze waren er al lang. Internet maakt het alleen zichtbaarder. Ook de slechte beveiliging van operating systems in pc's wordt versterkt. Zolang pc's niet verbonden zijn aan het Internet valt het niet zo op, maar zodra ze verbonden zijn worden de lekken duidelijk en wordt de schuld aan Internet gegeven. We kunnen nog niet zo goed omgaan met het feit dat Internetzaken meer zichtbaar, en gelijk op wereldschaal, maakt. Daar wordt op dit moment paniekerig op gereageerd. Internet stelt op het punt van veiligheid problemen. Mensen kunnen versleuteld met elkaar communiceren waardoor ze niet meer zijn af te luisteren zijn. Vervolgens zijn er pogingen geweest, gelukkig tot nu toe onsuccesvol, om encryptie aan banden te leggen. Met als gevolg dat de burger geen encryptie gebruikt, maar de crimineel wel. Anderzijds zijn er enorm veel bronnen om opsporingsonderzoek te doen. Bij privacy zie je bijna het omgekeerde. Het is onbegrijpelijk hoeveel mensen van zichzelf vrijgeven op Internet. Ze zijn zich er niet van bewust of het kan ze niet schelen. Omgekeerd biedt Internet ook mogelijkheden om je privacy juist enorm te beschermen.
Ik denk dat Internet in 2030 niet meer door de maatschappij (of de oorspronkelijke ontwikkelaars) wordt vormgegeven, maar door de commercie. Het wordt een domein dat wordt overgenomen door commerciële bedrijven. Je kan steeds minder vrij van eindpunt naar eindpunt communiceren. Er komen steeds meer barrières in de vorm van intelligentie onderweg en gesloten protocollen. Vaak onder het mom van beveiliging en schaarste van *resources*. Killer-applicaties zijn daardoor steeds minder mogelijk, tenzij ze draaien bovenop het *worldwide web*, want dat komt door alle firewalls heen. Applicaties die naast het *worldwide web* draaien zijn steeds moeilijker te ontwikkelen. Ik voorzie een volledig gesloten Internet, vergelijkbaar met de telefoonsystemen (RL: vgl. Lessig's betoog in the

Future of Ideas). De meeste overheden vinden dit eigenlijk wel prettig, want dit biedt veel meer mogelijkheden tot controle. Vanuit de VN zijn er bijvoorbeeld discussies gestart, zoals in de 'Working Group on Internet governance' (WGIG), in het WSIS (World Summit on the Information Society). Die discussie wordt gedomineerd door ontwikkelingslanden die vinden dat er meer controle moet komen en zij vinden daarin een partner in de commercie. Gezamenlijk zouden ze wel eens met het Internet aan de haal kunnen gaan. Als dat gebeurt, dan zouden er wellicht twee netwerken naast elkaar kunnen ontstaan: het gesloten commerciële netwerk met prachtige diensten en *quality of service*, volledig gecontroleerd, en waarbij je niet weet wat er met je gegevens gebeurt, en een open netwerk dat de ideeën van de oorspronkelijke ontwikkelaars: vrije communicatie tussen iedereen, honoreert. Dit laatste net zal echter, denk ik, een marginale rol spelen ten opzichte van het grote geheel. Zelfs als Nederland zou willen is daar moeilijk aan te ontkomen door internationale afspraken. Het is steeds minder mogelijk een stap terug te doen en na te denken over wat willen we met, bijvoorbeeld, auteursrecht en nieuwe media. Op grond van internationale ontwikkelingen worden we in een bepaalde richting geduwd, technische voorzieningen (DRM) en afkalving van privacy. De lobby vanuit de commercie is veel sterker dan het maatschappelijke bewustzijn.
Consumentenorganisaties en burgerrechtenbewegingen zoals EFF en BoF, proberen wel tegengas te geven maar hebben nauwelijks achterban.
Ik verwacht niet dat jeugdige P2P-gebruikers het illegale uitwisselingssysteem op zullen blazen. Die gaan vanzelf volwassener gedrag vertonen en zich aan de regels houden. Wat ik wel verwacht is dat ze, omdat ze kennis hebben van de mogelijkheden, zich in hun werk als, bijvoorbeeld, wetgevingsambtenaar, minder laten leiden door de mooie praatjes van de commercie.
Internet speelt een belangrijke rol bij **vergrijzing**. De vergrijzing komt door de babyboomers. Deze zijn tamelijk goed bekend met Internet. Mensen krijgen meer tijd en zullen meer tijd op Internet besteden. Kijkend naar mijn eigen omgeving dan lijkt het er op dat ouderen meer behoefte hebben aan veiligheid en minder aan privacy.
Veiligheid en privacy, of eigenlijk veiligheid en vrijheid, staan vrijwel altijd op gespannen voet met elkaar, waarbij vrijheid is gekoppeld aan privacy. De balans is belangrijk. 'Those who sacrifice freedom for security deserve neither security nor freedom.' We geven op dit moment te veel moeizaam opgebouwde rechten op ten gunste van vermeend hogere veiligheid. Het systeem van checks en balances wordt afgebroken. Voorlopig zal dat wel goed gaan, maar op een gegeven moment wordt er misbruik gemaakt van de vergaarde gegevens en dan is het ontbreken van de checks en balances funest voor zowel je vrijheid als je veiligheid. De **rol van de overheid** is het bewaken van de balans van vrijheid, beveiliging en privacy. Maatregelen ter verhoging van de veiligheid moeten zeer weloverwogen worden genomen en dat gebeurt op dit moment in de VS niet. In beide scenario's speelt de overheid dezelfde rol. Privacy en veiligheid zijn onlosmakelijk met elkaar verbonden. De overheid moet de juiste balans bewaken. Een voorbeeld van hoe het niet moet is het aan de ene kant hebben van een zorgvuldig opgezet dataprotectieregime in Europa, maar dan vervolgens gemakkelijk passagiersdata overleveren aan de VS op een manier die duidelijk niet strookt met het Europese beschermingsniveau. Dan ben je weinig bewust met beleid bezig.
Bewaren van gegevens is niet te stuiten. Dat levert een enorme kostenpost op, in eerste instantie voor ISP's, maar die berekenen het uiteraard door naar de consument. Het is bovendien kwetsbaar. Het is te hopen dat het afgeschermd is, maar je kan wachten op misbruik, onder meer van binnenuit. Beveiligen wordt lastiger en het net wordt kwetsbaarder doordat de infrastructuur moet worden aangepast om aftappen mogelijk te maken bij de Internettechnologie van *packet switching*. De neveneffecten zijn enorm en tasten de privacy sterk aan.
Ik geloof dat gevoelens van bescherming van de privacy in Europa ervoor zorgen dat cameratoezicht (**surveillance**) beperkt zal zijn (zeker ten opzichte van de VS). Op de werkplek en in private omgevingen zullen camera's niet worden omarmd. In de openbare ruimte zullen ze wel oprukken. Ook in de bejaardenzorg zie ik meer camera's verschijnen. De balans veiligheid-privacy valt hier anders uit dan elders. **Gated communities** zie je vooral in derdewereldlanden (wegens grote inkomensverschillen) en in de VS. Maar zelfs in Nederland sluit ik het niet uit. Interessant is dat de veiligheid van de openbare ruimte hierdoor afneemt. De veilige ruimte wordt in zo'n geval beperkt tot de gesloten *community*. Ik hoop dat maatregelen op basis van de afweging veiligheid-privacy en vrijwilligheid worden genomen.
Iedereen zal worden opgenomen in **DNA-databanken**, denk ik. De gevaren zijn duidelijk, maar de checks en balances zijn eenvoudiger in te bouwen dan bijvoorbeeld bij inbouw van camera's in de huiselijke sfeer.
Een belangrijke bescherming van privacy is het feit dat informatica nog niet erg ver is met betrekking tot bijvoorbeeld **datamining**-technieken. Als databanken goed zijn te koppelen met bijvoorbeeld *Artificial Intelligence*-technieken, dan is profilering en volgen van gedrag mogelijk en zal het bedrijfsleven hier op grote schaal gebruik van gaan maken. Denk in dit verband bijvoorbeeld aan Doubleclick, dat op veel websites advertenties heeft, en dat nu al het surfgedrag van veel surfers kan volgen doordat de advertentie*banners* van hun servers worden geladen en zij dus zicht hebben op de pagina's die een bepaalde surfer bezoekt. Commerciële partijen zoals deze weten binnenkort veel meer van burgers dan de KGB ooit deed, en aangezien het via het laden van advertentieplaatjes gaat valt het grotendeels buiten het bereik, of in ieder geval het zicht, van de privacyregelingen.
Tennet van de CIA heeft net verkondigd dat Internet alleen toegankelijk moet zijn voor gecertificeerde personen om misbruik te voorkomen. Dat zou kunnen leiden tot een afsluiten van het Amerikaanse Internet van de buitenwereld. Dat zijn verstrekkende maatregelen ter vergroting van de veiligheid. Dit soort discussies lopen. In tegenstelling tot een paar jaar geleden moeten we dit soort signalen serieus

nemen, er gebeuren nu meer dingen die we niet voor mogelijk hielden. Binnen ICANN is bijvoorbeeld ook besloten om de *root DNS-server* die oorspronkelijk in de VS stond te klonen op meerdere plaatsen buiten de VS om VS-dominantie iets te beteugelen.
Informationele privacy wordt verder aangetast in de toekomst. Dichter bij het individu komende privacyinbreuken, zoals fysieke inbreuken en het monitoren van gedrag, zullen minder sterk worden beperkt, aangezien mensen daar gevoeliger voor zijn. Dat laat onverlet dat er veel vormen van onzichtbare monitoring zijn (RFID). Ik mag hopen dat we kinderen en ouderen niet gaan uitvoeren met dergelijke chips. Aan de andere kant is de identificatieplicht betrekkelijk eenvoudig doorgevoerd. De stap naar chipimplantatie bij de geboorte is daarmee dichterbij gekomen. Ook in paspoorten (de VS voorop) gaan RFID-chips komen. De primaire doelstelling daarbij is denk ik het heimelijk kunnen uitlezen van deze data. Daar moet naar mijn idee een diepgaande discussie over worden gevoerd, maar helaas wordt dit soort beslissingen steeds meer genomen op een niveau waarop we er in Nederland helemaal geen invloed op kunnen uitoefenen.
Anoniem surfen lijkt me in 2030 uitgesloten. Je kunt anoniem opereren, maar opsporing zal altijd de bevoegdheid hebben om gegevens op te vragen bij bijvoorbeeld ISP's.
Waar ik me zorgen over maak is het verdwijnen van programmeerbare *general-purpose devices*. Ik voorzie dat programmeerbare *devices* zullen worden verboden en dat er alleen specifieke devices zijn die precies doen wat de *contentproviders* willen. Meer grip van commerciële partijen en overheden.

Vraaggesprek met Ulco van de Pol

Bert-Jaap Koops, 30 november 2004

Ulco van de Pol is plaatsvervangend voorzitter van het College Bescherming Persoonsgegevens.

Veiligheid in 2030 betekent, naast klassieke veiligheid, een groter belang van informatieveiligheid. Nu nog heeft men een groot geloof in moderne technieken, in de toekomst zal meer aandacht zijn voor onveilige situaties die ontstaan door toenemende informatiegerelateerde techniek, zoals heimelijke waarneming (denk aan RFID) en profilering. Ook van een ontwikkeling als verplichte bewaring van gegevens, zoals die nu wordt besproken voor verkeersgegevens, verwacht ik zeker dat die zich doorzet naar andere sectoren, zoals bij cameratoezicht en banken, die steeds meer gegevens moeten verzamelen. Deze tendens zal, zo hoop ik, alleen in bedwang worden gehouden door de kosten ervan en door de vertrouwensrelatie die moet bestaan tussen overheid/bedrijf en burger/klant.
Bij **techniek** denk ik vooral aan convergentie van communicatiesystemen, waar we ons meer en meer aan overleveren. Zie het voorbeeld van Gmail (http://gmail.google.com/gmail/help/about.html) dat inhoudsgerelateerde advertenties toont bij e-mail. Je wordt steeds meer geleid door techniek, de mogelijkheid je eraan te onttrekken neemt af. Dat kan ook gaan spelen bij robot-achtige toepassingen, niet als autonome systemen, maar als comfortabele gidsen, bijvoorbeeld in het verkeer. Techniek zal meer beslissingen voor ons nemen; daar zit een spanningsveld in tussen enerzijds overgeven aan gemak en anderzijds controle kunnen houden. Bovendien neemt de *ongemerkte* waarneming toe; kijk naar de OV-chipkaart die die mogelijkheid zou kunnen bieden, en de winkel van de toekomst die volop klanten kan profileren. Belangrijk is het punt waarin dienstverlening omslaat in dwang.
Privacy betekent in 2030 niet per se afscherming; we moeten af van de indruk dat privacy vooral afscherming beoogt, we krijgen steeds meer last van het begrip privacy in dat opzicht. Het betekent eerder zicht houden op en zeggenschap hebben over informatie en gegevens. Het gaat om autonoom kunnen functioneren en keuzes kunnen maken; privacy is in dit opzicht een deelaspect van die autonomie. Informationele privacy zal in 2030 het meest onder druk staan, dus daarvoor is maximale aandacht nodig. We hebben daartoe spelregels nodig voor de informatiehuishouding, en we moeten er vooral voor zorgen dat in dit opzicht de informatie-infrastructuren aan de maat en onder controle zijn. Dat kan bijvoorbeeld door consequent als standaardinstelling te hanteren niet wat maximaal mogelijk is, maar wat minimaal nodig is – een vorm van PET. Een ander wezenlijk aandachtspunt is doelbegrenzing. Bij de informatietechniek nu en in de toekomst ligt een heel breed gebruik op de loer; er is sprake van een erosie van het noodzakelijkheidsbegrip, waardoor de doelbegrenzing vervaagt en de mogelijkheid greep te houden op gegevens kleiner wordt.
Naast de gegevensbescherming duidt privacy ook op een algemener begrip, een cultuur- of **beschavingselement**. Daarbij staan we nu op een kritiek punt om dit element overeind te houden; de huidige trend is meer dat je moet uitleggen aan de maatschappij waarom je iets wilt afschermen, in plaats van het omgekeerde dat we van oudsher associëren met dit beschavingselement. Hierbij gaat het vooral om de verschillende maatschappelijke rollen die mensen vervullen en de sociale afgrenzingen in de maatschappij; als je niet meer kunt scheiden wie je bent als bijvoorbeeld werknemer, verzekerde en patiënt, lig je open en bloot en kun je niet meer autonoom functioneren.
Wat **ruimtelijke privacy** betreft, verwacht ik dat de maatschappij beheerst zal worden door waarnemingssystemen. De behoefte aan een eigen afgeschermde plek ('My home is my castle') zal toenemen. Mogelijk worden eilandjes gecreëerd in de vorm van *compounds*, waardoor de controlebehoefte zal toenemen. De voordeur schuift daarbij op: er zal gevochten worden wie de baas is in het grijze gebied tussen huisvoordeur en *compound*grens. De controle van de publieke ruimte zal echter grotendeels publiek kunnen zijn; ik ben blij met de huidige tendens dat het publieke domein door de overheid ook weer als publiek domein wordt gezien waarop de overheid moet toezien. Daarbij is wel van belang dat we ook controle moeten inbouwen op de controleurs: mensen lijken nu een volstrekt naïef geloof te hebben dat we degenen die ons controleren ook onverkort kunnen vertrouwen.

Lichamelijke integriteit vind ik minder belangrijk, althans vanuit privacy-oogpunt. Wel belangrijk is **genetische informatie** die uit het lichaam kan worden gehaald; dat is een zeer belangrijk aandachtspunt. Te verwachten valt dat de maatschappij zal eisen dat informatie over genetische aanleg ook buiten de zorg beschikbaar komt, en dat het afleiden van dergelijke informatie ook heimelijk zal gebeuren. Screening op dergelijke informatie gebeurt nu al; ik verwacht dat dit alleen maar zal toenemen, bijvoorbeeld door profielen te maken van agressie wanneer dat technisch mogelijk is, en het gedrag van mensen met 'agressiegenen' te monitoren. Vergelijk de huidige verwijsindex voor jeugdige potentiële criminelen (een soort 'boefjesbank'), waarvan het eerste meldpunt de zuigelingenzorg is (!). Een groot zorgpunt daarbij is dat het gaat om verwachtingen en niet om zekerheden, en om profielen in plaats van om de individuele, autonome persoon. Een gerelateerd voorbeeld is de forensische DNA-databank, die naar mijn verwachting sowieso zal uitbreiden. In een veiligheidsmaatschappij in 2030 zal de hele bevolking daar in zitten, waarbij ook risicoselectie zal worden toegepast; als de maatschappij meer een privacymaatschappij is, zal de DNA-databank niet bevolkingsbreed zijn, maar nog steeds uitgebreider dan nu – ook hier verwacht ik een erosie van het noodzakelijkheidsbegrip.
De **rol van de overheid** in een privacymaatschappij is denk ik een klassieke: de overheid waarborgt bescherming van burgers. In een veiligheidsmaatschappij zal de overheid veeleer ook *uitvoerder* zijn van tal van maatregelen om veiligheid te waarborgen, en daarbij ook nauw toezicht houden op andere uitvoerders. Ten aanzien van de rol van burgers bij de opsporing van strafbare feiten in 2030 heb ik niet zo'n beeld; we moeten vooral niet doorslaan naar een politiestaat (model Stasi-archief). Het cultuurverschil tussen Oost-Europa en West-Europa is in dat opzicht treffend; in West-Europa hebben we een veel groter – ik denk: te groot – vertrouwen in de overheid. En we moeten ook oppassen voor een verklikkersmaatschappij, waarin men een grote scheiding aanbrengt tussen boeven en brave burgers; zo'n scheiding valt helemaal niet zo scherp te maken.

Vraaggesprek met Arie Rip

Rachel Poels, 10 december 2004

Arie Rip is sociaal-wetenschappelijk onderzoeker op het gebied van wetenschap en techniek.

Technologie
Arie Rip vindt dat er twee specifieke zaken belangrijk zijn als het gaat om de ontwikkeling van de technologie in de toekomst. Ten eerste voorziet Rip een gedistribueerde en daardoor veel flexibelere technische infrastructuur. Daarnaast verwacht hij verdergaande miniaturisering waardoor veel meer mogelijkheden gecreëerd zullen worden. Dat speelt al in de klassieke sectoren als chemische industrie, als brandstofcellen locaal energie kunnen produceren om reacties te laten verlopen. "Neem nu het voorbeeld van de *Ambient Intelligence*, dat kan nog een aantal stappen verder gaan in termen van entertainment, met name als batterijen of andere energiebronnen kleiner en sterker worden.En je ziet tegelijkertijd een soort van cyborgachtige-ontwikkeling waarin heel veel techniek in of aan het lichaam en de kleren zit." Rip ziet veel kansen voor de ontwikkeling van cyborg-achtige technologie. Daarmee doelt hij echter niet op het verbeteren van mensen. "Ik zie het meer als een samenstel van allerlei gadgets en implantaten. Een veel meer samengestelde functionaliteit. Bij de *human enhancement business* krijg je heel erg het verhaal: 'Zo moeten we allemaal worden'. 'Zo gaan we nieuwe mensen maken'. Volgens mij is het nog gewoon de oude mens, maar met wat meer handigheidjes. En dus redelijk wisselend opgebouwd. Het is niet gebaseerd op menselijke tekortkomingen die moeten worden gecompenseerd door de techniek, maar het heeft te maken met gadgets, die natuurlijk wel dingen kunnen *enhancen*. Als het gaat om het koppelen van ICT aan zenuwen, daarvan denk ik niet dat het er zal komen. Het zal hem meer zitten in het feit dat je veel meer weet van neuro-chemie en dat je daardoor ook eigen gedrag kunt beïnvloeden."

Rip vermoedt dat tegen 2030 de genomics-hype al wel voorbij zal zijn. "Die belofte van individuele diagnose en individuele DNA-signatuur; dat lijkt me ten onder gaan aan fouten en risico's op fouten die optreden in al die analyses en diagnoses. De ontwikkeling gaat nu nog wel door en dat is misschien ook nog wel gerechtvaardigd. Maar voor gerichte therapie, patiëntenpaspoorten en dat soort dingen is nodig dat voldoende onderzoek gedaan kan worden naar de relatie tussen specifieke DNA en ziektebeelden. Daar kunnen gewoon niet genoeg gegevens voor verzameld worden om dat ooit voor elkaar te krijgen. Daarom is deze belofte van genomics een hype, dat klapt in elkaar tussen de 5 en 10 jaar na nu. (Wat je wel meer zult hebben is *point of care*-diagnostiek. Dingen meten zoals lichaamsvloeistoffen; dat kan allemaal kleiner en sneller.)
Ik denk dat je wel een herwaardering krijgt van datgene wat je in je genetische make-up nu eigenlijk bent en wilt." Bij de mensen die zich bezig houden met genomics is inmiddels al wel duidelijk dat het niet de genen zijn die bepalend zijn, maar dat het de co-evolutie is in combinatie met de omgeving, stelt Rip. Echter, in de algemene beeldvorming heerst nog steeds het beeld dat het de genen zijn die 'het hebben gedaan'. "Als dus de genomics-hype inklapt, dan gaat dit beeld ook wankelen. Dan kun je er niet meer omheen dat het een te eenzijdig beeld was en dat kan betekenen dat je in de maatschappij en in de opvoeding tot andere dingen gaat komen." Volgens Rip is het zo dat de techniek in eerste instantie bepaalde beelden in stand houdt, maar als er technologische veranderingen komen, dat die bestaande beelden dan kunnen ineenklappen en dat dan op allerlei plaatsen in de cultuur dingen gaan verschuiven.

Dat wil niet zeggen dat de maatschappij ondertussen niet wat zal gaan doen met de kennis van de genen waar het gaat om zaken als agressie, gebrek aan normbesef en andere misdaadgerelateerde

kenmerken. "Het zal wel geprobeerd worden hier en daar. In Amerika willen ze het graag, maar er zijn ontzettende tegenkrachten. Ik zie het zelf als een ongefundeerde zaak om dat soort combinaties te maken." Wat er zal gebeuren is dat we ons een paar keer lelijk in de vingers zullen snijden doordat op basis van genetische kenmerken bepaalde prognoses en verwachtingen worden gecreëerd. "Daarna zal het wel weer wegzakken. Maar, ondertussen zijn er wel slachtoffers gevallen. Onschuldige veroordeelden. Het kan een *self-fulfilling prophecy* zijn: als je door iedereen voor agressief wordt uitgemaakt, daar word je wel agressief van. Maar – om misverstanden te vermijden – ik wil niet zeggen dat er dit soort ontwikkelingen zúllen zijn. Ik zeg er steeds bij, dit kán een bepaalde richting opgaan. Verder denk ik dat ontwikkelingen nooit voor de hele maatschappij dekkend zullen zijn. Het is steeds een lappendeken. Dat is het verhaal dat ik uitzend."

Privacy

Privacy heeft Rip altijd een raar begrip gevonden. Veel toekomst ziet hij er dan ook niet voor. "Ik kan me er niet zo heel veel bij voorstellen, behalve gewoon de *common sense*-betekenis van 'ik wil eventjes alleen zijn'. Het is voor mijn gevoel zo heel erg Westers, en binnen het Westen dan nog heel erg Engels/Amerikaans waarin het *public and private*-onderscheid heel erg sterk is, met het gevolg dat *private* het recht is om afgeschermd te zijn van *public* of interventie. Zo wordt privacy ook gedefinieerd in de debatten. Ikzelf zie privacy meer als iets wat af en toe voorkomt; niet een recht waar je voor moet vechten. Dus als je dat ook nog eens combineert met het feit dat de wereld demografisch zal veranderen in de loop van de toekomst, dan verwacht ik dat we naar een het Chinees-Japans model met een dosis India toe zullen gaan. Privacy is iets dat je voor veel geld kunt kopen. Dus als je vraagt hoe privacy er in 2030 zal uitzien dan is mijn *gut feeling*: de *hang-up* over privacy is dan voorbij. Misschien dat allerlei Noord-Amerikaanse actiegroepen het nog wel belangrijk vinden, maar dat ze dat doen hangt onder meer samen met eerdere demografie, onder andere de hele ontwikkeling van het uitgebreide gezin naar het kerngezin. Dat waren allemaal bewegingen in de richting van een ontwikkeling waarin privacy als een soort recht wordt gezien; een *entitlement* op privacy. En dat kan allemaal weer veranderen. Het is zeker geen onomkeerbare ontwikkeling."

Rondom het bewaren van gegevens verwacht Rip dat er een compromis zal komen. "Ik verwacht een wedloop waar het gaat om technieken rondom *security*; de terroristen versus de gezagshandhavers. Maar je kunt databestanden natuurlijk ook vervuilen; als je een e-mailadres moet opgeven, dan geef je olie.bol op of zo. En zo kun je ook andere dingen doen. Zoals websites te veel bezoeken waardoor je ze buiten werking stelt. Daar worden mensen ook steeds handiger in. Dat betekent dus dat de hele vraag naar de koppeling van databestanden een stationair niveau zal bereiken omdat die databestanden zelf niet zo handig meer zijn." Daarnaast voorziet Rip ook problemen met betrekking tot de opslag van die gegevens. "Het kan allemaal wel aan opslagruimte, maar het is een toegangsprobleem. Je kunt misschien al die archieven nog wel hebben, maar als je niet weet hoe je bij gegevens die je nodig hebt moet komen."

Veiligheid

Als het om veiligheid gaat en de vraag wat veiligheid in 2030 kan inhouden, vertelt Rip dat hij er een soort basisfilosofie op nahoudt: "Ik heb het idee dat de wereld chaotisch is en dat er af en toe met heel veel moeite en energie orde in stand gehouden wordt. Ter illustratie daarvan: ik vind een aantal dingen die nu gebeuren een beetje op inklappen lijken. Als je de reacties van nu ziet, die doen me erg denken aan 1900 met de anarchisten en allerlei andere bewegingen in Europa. Dan heb ik zoiets van 'nou, het zal nog een verdere chaos worden'. Dan kun je een aantal *pockets of security* krijgen, wat je nu al lokaal in steden ziet: een wijk die helemaal afgeschermd is. Dat is veilig zolang de afscherming werkt. Dat is de eerste 10 tot 15 jaar. Maar dan is het de vraag wat er daarna gaat gebeuren. Ik denk dat er sprake is van bepaalde 'vorken' in de geschiedenis. Het kan zo zijn dat er meer discipline, energie en orde zullen komen en dat het dus een soort van jaren '50-veiligheid is. Al dan niet gecombineerd met spanningen zoals de hele kernbewapeningsspanning; daardoor leken en waren alle dingen ordelijk. Zo kan het dus in 2030 zijn. Maar het kan ook dat het allemaal nog maar verdere ellende is. En dat je inderdaad van die sciencefictionachtige verhalen krijgt van die *gated communities* en daartussen een onderwereld boven de grond. In mijn *gut feeling* vind ik dat het meest waarschijnlijke, maar ik heb er geen argumenten voor."

Rip verwacht dat de ontwikkelingen binnen de maatschappij wel in een richting zullen gaan waarin *surveillance* alomtegenwoordig zal zijn, maar hij verwacht ook hier dat gecentraliseerde *surveillance* uiteindelijk niet volledig realiseerbaar zal blijken. "Ik denk dat het toch waarschijnlijk vrij heterogeen blijft. De ene keer de ene camera, de andere keer een andere camera. Ik denk dat mensen het ook helemaal niet zo erg zullen vinden. Ik denk dat centrale *surveillance*, monitoring en het controleren daarvan uiteindelijk zichzelf verslaat, in die zin dat het heel veel inspanning zal vergen. Het is ook maar de vraag of het voldoende oplevert. Er is een richting naar meer centralisering, maar daarin moet je investeren. Dat moet je in stand houden en daarnaast komt er ook niet altijd veel uit. Dat vergt een grote inspanning. En op bepaald moment krijg je een soort van implosie; dan wordt het niet meer bijgehouden, verliest het zijn functies en dan zijn er kleinere databestanden die ineens weer dingen gaan overnemen. Buurtbewakingscomités in plaats van een centrale politiewacht. Daarop zal dan weer een beweging naar meer centralisering volgen. Ik denk dus dat het een heen-en-weerbeweging is in plaats van dat het een specifieke kant opgaat en zo blijft."

Nanotechnologie zal – als *enabling* technologie – via wat daardoor mogelijk wordt ook gevolgen hebben voor de veiligheid. "In ontwikkelingslanden zal het veel gemakkelijker zijn om lokaal dingen te produceren, bijvoorbeeld chemische producten die niet meer een grote installatie nodig hebben waar

alle temperatuur en druk geoptimaliseerd moeten worden. Voor terrorisme biedt dat andere mogelijkheden. Je kunt nu meer in termen van het maken van speciale chemicaliën. Er zal een nieuwe interesse komen in chemische oorlogsvoering. Dat is wat in de nanotechnologieverhalen een beetje weggedrukt is, deze route van ontwikkeling ten opzichte van die van de *human enhancement*. Ook daarbij gevolgen voor de *security*. *Human enhancement* is iets waaraan überhaupt veel *security*-problemen vast zitten. Er zal een nieuwe versie komen van *gated communities*. De *enhanced humans* tegenover de *non-enhanced humans*. Wat veiligheidsproblemen zal opleveren, want *enhanced humans* zullen een extra reden hebben om in *gated communities* te verblijven."

Wat Rip niet ziet gebeuren is dat iedereen in de toekomst verplicht een chipje in zijn of haar lichaam zal dragen. Met betrekking tot gevangenen kan hij zich er echter wel wat bij voorstellen. "Dat zal wel gebeuren als een soort deal; je mag wat meer vrijheid als je een chip in laat brengen, maar dat gebeurt toch al. En daarnaast denk ik dat het ook gebruikt zal worden in bedrijven en in supermarkten. Het zal niet zo zijn dat er een streepjescode komt voor iedereen. Ik zie het zelf meer opkomen in verschillende domeinen met een eigen dynamiek. Zie nu al de Verichip voor nachtclubbezoekers (o.a. in Barcelona). Het zal niet universeel zijn. Zulke doembeelden zijn overigens niet verkeerd. Doembeelden stemmen tot nadenken en eventueel tot tegenreacties waardoor het geen *self-fullfilling prophecy* wordt. Mijn verhalen zijn wat dat betreft veel te reflexief. Ik zeg dat zal niet zo'n vaart lopen. Maar jehebt juist dit soort acties en reacties nodig om het niet zo'n vaart te laten lopen."

De vergrijzing en maatschappelijke ontwikkelingen

Ook de vergrijzing zal veranderingen brengen voor de toekomst, meent Rip. Je moet je alleen wel afvragen of die vergrijzing zich nog zo zal doorzetten als nu het geval is. "Als die vergrijzing zo doorgaat dan zal de hele zorgsector gaan schuiven. Wat je nu in Nederland heel sterk ziet, is dat er ten dele sprake is van een ontwikkeling waarin teruggegaan wordt naar de situatie als in de jaren voor 1950. Toen was zorg een zaak van familie en buren en de kerk. Daarnaast zal er sprake zijn van een opkomst van privé-klinieken en centra voor diagnose waar je – als je voldoende mobiel inclusief financieel onafhankelijk bent – van alles kunt laten doen. Wat ik niet helemaal zie, maar wel hoop, is dat bepaalde vormen van euthanasie gangbaarder worden. Dat er op een gegeven moment over het leven gedacht gaat worden in termen van 'ontplooiing en voltooiing'. Een voltooid leven. Ik hoop dat dat een veel nadrukkelijker onderdeel van de cultuur wordt. En daarnaast denk ik dat de hele genomics*bubble* en de *aftermath* daarvan daar ook een effect op kunnen hebben. Als dat idee van 'ik word geleefd door mijn genen' verdwijnt, dan ga je inderdaad denken in termen van 'ontplooiing en voltooiing'. Dat wordt dan in onze cultuur een veel natuurlijker onderdeel. Het hangt ook samen met de merkwaardige positie van de medici. Die hebben nu een soort alleenrecht op medisch handelen. Euthanasie wordt gedefinieerd als medisch handelen. Op het moment dat je aan de diagnosekant veel meer dingen krijgt – *point of care*-achtige zaken – dan wordt de rol van de arts anders. Dan kan het zo zijn dat de vraag wie bepaalde handelingen verricht verandert. Als dat eenmaal opengegooid is, zal dat verschuivingen van de acceptatie van verschillende handelingen teweeg brengen. Dat is een culturele verandering. Daar zitten op allerlei plekken wel technische stapjes in. Echter, die geven niet als zodanig deze richting aan, maar ze leveren wel verschuivingen op die de beroepssituatie van de medici verandert."

Het laatste woord

Rip gelooft niet dat je privacy en veiligheid als twee verschillende – tegengestelde – grootheden tegenover elkaar moet zetten in de zin van 'meer security betekent minder privacy'. "Als je scenario's op een dergelijke manier opbouwt dan gaat er iets mis. Je moet namelijk een complexiteit kunnen laten zien. Het punt dat in mijn verhaal de hele tijd zat is dat er een soort co-evolutie is tussen techniek en maatschappij. Je moet het meer aanpakken als een romanschrijver: hoe zouden die dingen kunnen gaan? Wat ik zelf heel graag doe in mijn scenario's is niet het schrijven van uitgewerkte werelden, maar vorken in bepaalde scenario's. Zo van 'daar ligt een cruciale vertakking', als je eenmaal heel specifiek de ene kant op gaat, is het heel lastig om weer terug te gaan."

Bijlage II. Samenvatting van inbreng via de webvragenlijst

In de periode november 2004 – december 2004 is een online vragenlijst met acht open vragen beschikbaar geweest. Door middel van gerichte uitnodiging naar geselecteerde personen uit wetenschap en publieke sector, heeft de onderzoeksgroep om – anonieme – reacties gevraagd ter aanvulling op de diepte-vraaggesprekken (bijlage I). Uiteindelijk is de vragenlijst ingevuld door 17 personen. Een analyse van de antwoorden levert de volgende beelden op.

1. Hoe denkt Nederland over veiligheid in 2030?
Door verschillende respondenten wordt een tendens richting privatisering van de bescherming van de veiligheid voorspeld. Er wordt een bloeiende markt voor private veiligheidsbedrijven voorzien die gehoor moet geven aan de veiligheidsbehoefte in een maatschappij die zich kenmerkt door zelfredzame burgers. Dit laatste wordt ingegeven door een feitelijke onmacht van de staat om het gewenste niveau van veiligheid te bieden. De inhoud van het concept veiligheid wordt in toenemende mate bepaald door Europa.
De veiligheid is steeds meer alleen te garanderen in betrekkelijk kleine omgevingen: de buurt, het uitgaansgebied, de winkelstraat. Daarbinnen geldt een sterk geobserveerde, betrekkelijk veilige wereld, daarbuiten een onbeschermde onveilige wereld.

2. Wat bedreigt de veiligheid in 2030?
De voornaamste genoemde bedreigingen zijn: een toenemende kloof tussen rijk en arm, waarbij rijk zich steeds duidelijker als rijk manifesteert, terrorisme, intolerantie en bedreigingen van de leefwereld in de vorm van overbevolking, schaarste van water en grondstoffen en natuurgeweld.

3. Hoe denkt Nederland over privacy in 2030?
Een meerderheid van de respondenten schetst een beeld waarin privacy ondergeschikt is (geworden) aan veiligheid. Burgers offeren hun privacy welwillend op ten gunste van (een vermeend gevoel van) veiligheid. Met name *surveillance* en *monitoring* als middelen om de leefomgeving veiliger te maken worden hierbij genoemd als inbreuken op de privacy. Sommige respondenten voegen aan deze ontwikkeling toe dat we op een zeker moment wellicht tot de ontdekking zullen komen dat te veel privacy is opgeofferd.
Tegenover de respondenten die privacy het onderspit zien delven ten faveure van veiligheid staan respondenten die stellen dat de veiligheid juist gebaat is bij meer privacy. Ook wordt gesteld dat er bewegingen zijn die duiden op een wens van burgers tot versterking van hun recht 'to be let alone', getuige bijvoorbeeld de wens om spam aan te pakken. Privacy wordt door een enkeling ook aangeduid als verhandelbaar recht.

4. Wat bedreigt privacy?
De grootste bedreiging van de privacy wordt volgens de respondenten gevormd door de opsporings- en inlichtingendiensten die enerzijds bevoegdheden naar zich toe trekken en anderzijds ook bevoegdheden krijgen aangereikt door gekozen volksvertegenwoordigers die niet bij machte zijn een gedegen afweging te maken tussen de verschillende belangen.
Verder worden ook de markt, en dan met name grote multinationals, genoemd als grote verzamelaars van persoonsgegevens. ICT wordt in dit licht genoemd als katalysator, terwijl ook (misbruik van) het Internet als risico wordt genoemd. Een enkeling ziet vrijheid als grootste bedreiging, terwijl een ander privacy in dit zelfde perspectief bestempelt als concept van het vrijheidsdenken uit de jaren '70 dat is verworden tot onverschilligheid voor anderen.

5. Is privacy een bedreiging voor veiligheid of vice versa?
In de reacties komen duidelijk twee opvattingen naar voren. In de ene worden privacy en veiligheid niet als tegenpolen beschouwd, maar wordt het lot van beiden juist met elkaar verbonden: privacy bestaat niet, en is niets waard, zonder veiligheid en vice versa. De andere opvatting stelt dat veiligheid een bedreiging is voor privacy: om (het gevoel van) onveiligheid te bestrijden zullen burgers bereid (moeten) zijn steeds meer van hun privacy op te offeren.

6. Wat vindt u de belangrijkste ontwikkelingen in techniek en samenleving die onze veiligheid de komende decennia zullen beïnvloeden?
Op maatschappelijk vlak wordt het terugtrekken van mensen in beschermde omgevingen ('cocooning in gated communities', bijvoorbeeld) als bedreiging genoemd voor een open beeldvorming. Daarbij komt dat de rol van de media een sterkere invloed zullen hebben op deze beeldvorming. Of mensen in staat zullen zijn tot vrije en onbevangen beeldvorming wordt hiermee betwijfeld, hetgeen intolerantie en onverdraagzaamheid in de hand kan werken. Ook andere vormen van segregatie in wijken en buurten met een uniforme samenstelling naar ras, ethniciteit, sociale klasse en dergelijke worden als problematisch aangeduid.
Op technologisch vlak worden vormen van ICT-criminaliteit en ICT-terreur voorspeld die tevens een nieuwe vorm van kwetsbaarheid van de ICT-infrastructuur introduceren.
Een toenemende transparantie van burgers door middel van ICT (camera's, RFID) wordt eveneens voorzien. Verder worden genoemd ICT, intelligente huizen, Internet, een grotere kloof tussen rijken die zich beveiliging kunnen veroorloven en armen, en internationaal terrorisme.

7. Wat vindt u de belangrijkste ontwikkelingen in techniek en samenleving die onze privacy de komende decennia zullen beïnvloeden?
De mogelijkheden die ICT biedt om enorme hoeveelheden data op te slaan en te ontsluiten maakt dat het moeilijk wordt om te vergeten; hierdoor kunnen mensen moeilijk met een schone lei opnieuw beginnen. Verder wordt gesignaleerd dat van de opslagmogelijkheden en *monitoring*-capaciteiten van ICT gebruik zal worden gemaakt om meer en meer gegevens op te slaan, onder meer vanuit omnipresent cameratoezicht.

8. Overige suggesties
'Proficiat! Had u echt geen slechter tijdstip kunnen uitkiezen voor dit onderzoek? In deze periode weet u zelf toch ook wel welke antwoorden het hoogst zullen scoren? Of was dat nu net de bedoeling?

Bijlage III. Onderzoekers

TILT, Centrum voor Recht, Technologie en Samenleving
TILT bundelt het onderzoek van de Universiteit van Tilburg op het snijvlak van recht, ethiek en openbaar bestuur in relatie tot informatie- en communicatietechnologie en andere nieuwe technologie. De kerncompetentie is gelegen in de verbinding van fundamentele en grensverleggende wetenschappelijke inzichten met strategische vraagstellingen en ontwikkelingen op het gebied van recht, ethiek, bestuur en techniek. Binnen het centrum werken specialisten op het gebied van juridische wetenschappen, ethiek, bestuurskunde en techniek samen. Het onderzoek bestrijkt een breed terrein, waarin de hoofdthema's zijn: onderzoek naar de betekenis van ICT en informatisering voor informatiebetrekkingen en de regulering daarvan; onderzoek naar de betekenis van andere vormen van nieuwe technologie (op dit moment nanotechnologie en biotechnologie) voor recht en regulering; en de wisselwerking tussen recht, technologie en samenleving. Binnen ieder thema wordt zowel vanuit een fundamentele (onder meer promotieonderzoek) als vanuit een aan de praktijk gerelateerde invalshoek (contractonderzoek) onderzoek verricht.
TILT (tot medio 2004 werkzaam onder de noemer CRBI, Centrum voor Recht, Bestuur en Informatisering) heeft ruime ervaring met onderzoek op het gebied van privacy en veiligheid. Op het vlak van privacy en persoonsgegevens verschenen vele studies, evaluaties (van de Wpr) en dissertaties. Studies in opdracht van het Ministerie van Justitie onderzochten de opslag en het gebruik van politiële en justitiële gegevens en de maatschappelijke behoefte aan dergelijke gegevens en de informatieverzoeken van politie en justitie aan derden. Onderzoek werd verricht naar de vraag hoe burgers feitelijk denken over probleemsituaties waar belangen van opsporing en toezicht moeten worden afgewogen tegen individuele privacy, en seminars over afwegingen rond privacy en veiligheid werden georganiseerd met diverse doelgroepen. TILT deed veelvuldig onderzoek naar justitiële opsporingsbevoegdheden, de invloed van ICT op het strafrecht en de gevolgen van nieuwe technologie voor de opsporing, alsmede naar risico's in de netwerksamenleving en informatiebeveiliging.

Betrokken onderzoekers
Dr. **Bert-Jaap Koops** is universitair hoofddocent bij het Centrum voor Recht, Technologie en Samenleving (TILT, voorheen onderdeel van het CRBI) van de Universiteit van Tilburg. Hij doet onderzoek naar strafrecht en technologie, in het bijzonder opsporingsbevoegdheden en privacy, computercriminaliteit, cryptografie, informatiebeveiliging en DNA. Hij is ook geïnteresseerd in andere onderwerpen binnen het technologierecht, zoals identificatie, elektronische handtekeningen, digitale grondrechten, en algemene uitgangspunten van ICT-recht. Vanaf 2004 leidt hij een onderzoeksprogramma over recht, techniek en schuivende machtsverhoudingen. Koops is mederedacteur van het handboek Recht en Informatietechnologie en twee boeken over ICT-regulering, *Emerging Electronic Highways* (1996) en *ICT Law and Internationalisation* (2000). Zijn webpublicatie *Crypto Law Survey* wordt wereldwijd beschouwd als een standaardbron over cryptografie-regulering. In 2003 gaf hij gastcolleges aan de University of Dayton en George Washington University in de VS.
Koops studeerde wiskunde en algemene literatuurwetenschap in Groningen en werkte van 1994-1998 als AIO aan de Universiteit van Tilburg en de Technische Universiteit Eindhoven op het gebied van regulering van encryptie. Hij promoveerde in januari 1999 op het proefschrift *The Crypto Controversy*. In 2002 publiceerde Koops een boek over strafvorderlijk onderzoek van (tele)communicatie (Koops 2002); en onlangs verscheen van zijn hand een boek over de gevolgen in de nabije en de verre toekomst van nieuwe (opsporings)technieken voor de rechtsbescherming van woning en lichaam (Koops e.a. 2004). In de afgelopen jaren trad hij meerdere keren als dagelijks projectleider van onderzoeksprojecten op. Koops is voorts co-promotor van het begin 2005 af te ronden promotieonderzoek van Arno Smits naar aftappen van telecommunicatie.

Prof.mr. **Marc Groenhuijsen** is sinds 1987 als hoogleraar straf- en strafprocesrecht verbonden aan de vakgroep Strafrechtswetenschappen van de Universiteit van Tilburg. Hij promoveerde in 1985 cum laude op het proefschrift *Schadevergoeding voor slachtoffers van delicten in het strafgeding*, waarvoor hij in 1986 de Moddermanprijs toegekend kreeg. Groenhuijsen is tevens rechter-plaatsvervanger in de arrondissementsrechtbank te Rotterdam (1986-heden) en raadsheer-plaatsvervanger in het Gerechtshof te Arnhem (1992-heden). Verder is hij benoemd tot erelid van de Vereniging Landelijke Organisatie Slachtofferhulp (1995) en heeft hij diverse internationale toekenningen gekregen wegens bijzondere verdiensten op het gebied van slachtofferhulp, onder andere van het Hongaarse Parlement (1997), van de World Society of Victimology (2003) en van de National Organisation for Victim Assistance (2003, USA). Hij is redacteur (1983-heden, sedert 1993 hoofdredacteur) van het losbladige commentaar op het Wetboek van Strafvordering, lid (1990, sedert 1991-heden secretaris) van de redactie van *Delikt en Delinkwent* (voortzetting van Tijdschrift voor Strafrecht), lid (1991-heden en van 1994-2001 voorzitter) van het Executive Committee (Dagelijks Bestuur) van het European forum for Victim Services, voorzitter Raad van Advies van het Wetenschappelijk Onderzoek- en Documentatiecentrum van het Ministerie van Justitie (1995-2002).
Groenhuijsen is programmaleider van het lopende onderzoeksprogramma 'Nederlandse strafrechtspleging in Europa' van het Centrum voor Procesrecht. Hij leidde vele onderzoeksprojecten, waaronder een grootschalig onderzoek naar systematische grondslagen voor een nieuw Wetboek van Strafvordering ('Strafvordering 2001'), was promotor van enkele tientallen promovendi, en publiceerde over uiteenlopende onderwerpen in het straf(proces)recht in de vooraanstaande nationale en internationale tijdschriften. Zijn huidige onderzoek richt zich, naast de victimologie, onder meer op de invloed van Europa op het Nederlandse strafrecht en op *human security*.

Dr. **Ronald Leenes** is sinds 1 januari 2004 als universitair docent verbonden aan het Centrum voor Recht, Technologie en Samenleving (TILT) van de Universiteit van Tilburg. Zijn onderzoeksveld sinds begin jaren '90 is informatisering in het openbaar bestuur, (juridische) kennistechnologie en kennismanagement. Thema's in deze onderzoekslijn zijn: geïntegreerde publieke dienstverlening, intra- en Internettoepassingen als oplossing voor kennismanagementproblemen, herinrichting van de publieke dienstverlening en kiezen-op-afstand. Sinds zijn indiensttreding bij de Universiteit van Tilburg heeft Leenes zijn onderzoeksveld uitgebreid naar recht en technologie in het algemeen. Thema's in deze onderzoekslijn zijn: regulering van gedrag door middel van technologie ('code as code'), het gebruik van gegevensbestanden (registers) bij opsporing en vervolging, en computercriminaliteit en privacy. Recent heeft hij meegewerkt aan een internationaal onderzoek naar het gebruik van gegevensbestanden in opsporing en vervolging in het kader van een EU-project AGIS. Hij is projectleider van een juridische impactanalyse van de Overheidstransactiepoort (OTP) die momenteel in opdracht van het Ministerie van EZ wordt uitgevoerd.

Leenes studeerde Bestuurskunde aan de Universiteit Twente (UT) met als specialisaties bestuurskundig onderzoek en informatisering. Van 1989 tot 2004 was hij in verschillende functies werkzaam aan de faculteit Bestuurskunde. In januari 1999 is hij gepromoveerd op een proefschrift over *hard cases* in recht en rechtsinformatica. Hij heeft sinds 1994 aan de UT inleiding recht (strafrecht en privaatrecht) gedoceerd aan verschillende faculteiten binnen de UT en doceert sinds 1999 eveneens vakken op het gebied van ICT en recht, met aandacht voor strafrecht en ICT.
Leenes is Secretary/treasurer van de International Association of Artificial Intelligence and Law (IAAIL), secretaris van IFIP WG 8.5 en lid van COST Action A14 Working Group 3: 'ICTs and public administration', alsmede seniorlid van de Nederlandse Onderzoeksschool voor de Bestuurskunde.

Dr. **Miriam Lips** is als universitair hoofddocente bestuurskunde verbonden aan TILT, Universiteit van Tilburg. Sinds 1996 is zij werkzaam bij de Universiteit van Tilburg waar zij onderzoek verricht, doceert, publiceert en adviseert op het snijvlak van informatie- en communicatietechnologie (ICT) en de relatie tussen overheid en burger. Recentelijk heeft zij haaronderzoek uitgebreid naar nieuwe vormen van gepersonaliseerde publieke en private dienstverlening via nieuwe ICT en privacy management en identiteitsmanagement in elektronische relaties (bijv. e-government, e-health, e-shopping) vanuit een burger-perspectief beschouwd. Sinds maart 2004 is zij verantwoordelijk voor het sociaal-economisch onderzoek binnen het kader van het vierjarige Europese zesde kader project 'Privacy and Identity Management for Europe', een zogenaamd 'integrated project' waar 20 universitaire en industriële partners uit Europa en de VS een bijdrage aan leveren en waar de Europese Commissie een totale subsidie van 10,1 M€ aan heeft toegekend. Daarnaast is Miriam Lips onder meer eindredacteur van het onderdeel 'boek- en rapportbesprekingen' en lid van de redactieraad van het internationale tijdschrift 'Information Polity'; voorzitter (samen met professor John Taylor) van de permanente EGPA-werkgroep 'ICT in public administration'; lid van de IFIP-werkgroep 8.5 'Information Systems in Public Administration'; Academic Director van de TIAS-opleiding 'Master in Public Information Management'; lid van de Wetenschappelijke Adviesraad van het Bsik-programma 'Ruimte voor Geo-informatie'; en Senior Research Fellow van de Nederlandse Onderzoekschool voor de Bestuurskunde. Vanaf november 2003 is zij tevens als Visiting Fellow verbonden aan het Oxford Internet Institute, University of Oxford in Engeland. In het projectonderzoek van TILT levert zij vanuit haar achtergrond expertise op het terrein van de methodologie van sociaal-wetenschappelijk onderzoek, als ook domeinkennis ten aanzien van inrichting en functioneren van de politie-organisatie en de maatschappelijke beleving, kennis en behoeften ten aanzien van online privacy in de Europese samenleving.

Mr. **Rachel Poels** is promovendus bij het Centrum voor Recht, Technologie en Samenleving (TILT) van de Universiteit van Tilburg. Haar onderzoek richt zich op privacy en *identity management*. Daarnaast houdt zij zich bezig met vraagstukken op het gebied van privacy en nieuwe technologieën, zoals nanotechnologie en RFID (radio frequency identification).
Al tijdens haar studie journalistiek aan de Academie voor Journalistiek te Tilburg raakte Rachel Poels gefascineerd door nieuwe technologieën, het onderscheid tussen *science fiction* en *science fact,* en de juridische vraagstukken die daarmee samenhangen. Na het behalen van haar bachelorgraad in de journalistiek ging zij Nederlands Recht studeren aan de Universiteit van Tilburg met als specialisme Recht & Informatisering. In oktober 2004 behaalde zij haar meesterstitel met een scriptie over privacyvraagstukken in het licht van nanotechnologie. Gedurende haar studie journalistiek en in de daaropvolgende jaren werkte zij regelmatig als freelance journalist. Momenteel werkt zij als freelance journalist voor 2bcontent, een bedrijf dat onder meer gespecialiseerd is in het verzorgen van nieuws op het gebied van IT en Recht.

Mw. Prof. mr. **Corien Prins** is sinds april 1994 hoogleraar recht en informatisering bij TILT, voorheen onderdeel van het Centrum voor Recht, Bestuur en Informatisering, van de Universiteit van Tilburg en geeft leiding aan TILT. Corien Prins studeerde aan de Universiteit Leiden Rechtsgeleerdheid alsmede Slavische Taal- en Letterkunde. Ze was sinds 1986 werkzaam bij de Afdeling Recht en Informatica van de Universiteit Leiden. Na haar promotie in 1991 te Leiden, verbleef ze in 1993 een halfjaar als visiting professor aan Hastings Law School, San Francisco, USA. Prins is lid van het gebiedsbestuur MAGW van NWO alsmede lid van de programmacommissie van het NWO-stimuleringsprogramma ITeR (Informatietechnologie en Recht). Sedert 2003 is ze lid van de redactie van het Nederlands Juristen Blad (NJB). Daarnaast is ze lid van de redactie van Nederlandse tijdschriften (Privacy & Informatie; Computerrecht; Voorschriften Bescherming Privacy) en enkele internationale uitgaven (Electronic Journal of Comparative Law; Information & Communication Technology Law; International Computer Law). Onderzoeksthema's: regulerings- en normeringsaspecten van ICT en nieuwe technologie; vraagstukken rondom digitale identiteit en identificatie, anonimiteit en privacy, e-government en e-commerce, NGO's en Internet. In het verleden was Corien Prins projectleider van in opdracht van het WODC uitgevoerde onderzoeken (Sociaal-wetenschappelijke evaluatie van de Wet persoonsregistraties (1995) en een onderzoek naar art. 11 lid 2 van de Wet persoonsregistraties en informatieverzoeken van politie en justitie (1998-1999); van 2003 tot medio 2004 was zij voorzitter van de begeleidingscommissie bij het door het WODC uitgezette evaluatieonderzoek van de Wet bijzondere politieregisters.

Dr. **Anton Vedder** is universitair hoofddocent ethiek en recht bij de faculteit der Rechtsgeleerdheid van de Universiteit van Tilburg. De hoofdthema's van zijn onderzoek en onderwijs zijn: ethiek, recht en informatietechnologie, enerzijds, en ethiek, recht en internationalisering, anderzijds. Anton Vedder is voorzitter van het Center for Transboundary Legal Development en begeleider van verschillende onderzoeksprojecten. Het betreft hier onder andere twee promotieprojecten over privacy. Hij leidt interdisciplinaire projecten en programma's over ethiek, recht en Internet, over de WTO en over de legitimiteit van de macht van non-gouvernementele organisaties in internationale debatten over sociale en morele kwesties. Hij is lid van de interuniversitaire Onderzoeksschool Ethiek (KNAW-erkend), coördinator van het programmaonderdeel over Ethiek en ICT en lid van de Commissie Wetenschap. Hij is lid van het bestuur van het Platform Ethiek van de UvT.